Project Title:

App Safety – Unfiltered Access to Online Content Via Apps & The Risks it Presents

Cathal Murphy

James Finglas

Sean Guthrie

Department of Informatics
School of Informatics and Engineering
Technological University Dublin

Submitted to Technological University Dublin in Partial Fulfilment of the requirements for the degree of:
Bachelor of Science (Honours) in Computing

Supervisor: Mr. Arnold Hensman

Submission Date: 20/5/2019

Project Declaration Form

Group Members: James Finglas, Cathal Murphy & Sean Guthrie

Supervisor: Arnold Hensman

Course Co-ordinator: Mark Cummins

Module Name: 3rd year group project

Submission Date: 20-5-2019

We declare that the work contained in this report which we now submit on the programme of study leading to the award of Degree of Honours B.Sc. in Computer Science in Technological University for Dublin is our own work and has not been taken from the work of others. Any sources which have been referenced or analysed have been cited using the Harvard standard within the body of this report. It is entirely our own work except where otherwise stated and has not been submitted for assessment for an academic purpose at this or any other academic institution other then in partial fulfilments of the requirements stated above.

We have read and understood the Technology University Dublin's policy regarding plagiarism.

X _____

James Finglas

X _____

Cathal Murphy

X _____

Sean Guthrie

Acknowledgements:

- We would like to express our heartfelt thanks to Arnold Hensman, our Project mentor, without whose valuable insights and guidance this report research project would not have been possible. This is the second time we have had the pleasure of having Mr. Hensman guide one of our projects and keep our ship steered in the right direction and as before, he proved a superb, knowledgeable expert guide.

- We would also like to thank our course co-ordinator who from the very first day our third year in university, encouraged us to begin the project process regarding thinking about subject material, project focus and direction. He offered guidance and fair advice as well as constructive criticism regarding some of our initial project ideas. Indeed, it was Mr Cummins advice which ultimately helped shape our final project idea and for that we are extraordinarily grateful

- We would like to extend our thanks to CyberSafeIreland, who's tireless efforts on behalf of parents and teachers regarding increasing awareness of the risks associated with online safety, as well their efforts in producing such fantastic detailed report greatly aided us in narrowing our focus when conducting our own research. Their reports are thorough, conclusive and we hope to live up to their standard of professionalism, dedication and care with our own research and blog.

Abstract

The purpose of our research was to determine if there are risks related to unfiltered access to online content via Apps, particularly where children are concerned. This was our primary research question which we addressed by analysing previous research and confirming the results are still current and applicable to our target demo graph by conducting our own survey. Our research methods were quantitative in nature, and we feel the statistics prove such a risk does exist.

We conducted a feasibility study that determined that while services do exist to address the area of online safety, the area covering methods to reduce the risks involved is lacking.

We also conducted a case study to highlight some of the concerning areas surrounding unfiltered access to online content via Apps. This coupled with our initial research and feasibility study served to justify our project. We also felt that the existence of such services does not serve to impact on the feasibility of our project negatively and that in fact, our service would complement already existing services.

Our feasibility study found that in App settings are barely covered by any of the services recommended[1] by the Irish government. Our service addresses this by focusing specifically in app settings. We covered all the terms & conditions, important features and settings of each app, developed a safety rating system and developed a guide for each App that shows how to adjust the settings. Next, we offered up a best practice guide as to how we felt the settings should be adjusted to better reduce the user's visibility and online footprint and reduce the risks.

We designed a simple useable blog to deliver the information via WordPress. The aim of the website was to be as simple as possible while retaining a high level of usability and accessibility which we felt was lacking from quite a few of the recommended services put forward by the Irish Government.

Lastly, we drew our conclusions tying all our research together. Our conclusions determined there are risks related to unfiltered access to online content via Apps and that while services do exist that cover the area of online safety the specific area of in-App settings is inadequately covered. We provided a blog which fills this need by displaying all of our research relating to the risks of unfiltered access to online content via Apps simply and effectively.

Google analytics shall be plugged into our platform to allow for any future work we may wish to undertake once the core components of our project have been completed.

[1] There are 5 main resources offered up by the Department of Justice & Equalities Cybercrime website and of these the only resource to cover this topic is the website Webwise.ie. Neither Hotline.ie, the governments portal service BeSafeOnline, The ISPCC, NPC Primary or indeed, CyberSafeIreland (Ireland leading online safety charity) cover this topic. This websites coverage of this topic is well document and cited in our research, within the feasibility study section, as well as all of the other resources.

Contents

Project Declaration Form 2
Acknowledgements: 3
Abstract 4
1.0 Table of Tables 9
2.0 Table of Figures 10
3.0 Introduction 20
3.1 Motivation 20
3.2 Research Question 23
3.3 Project Goals 24
3.4 Summary 25
3.5 Methodology 28
3.6 Research Goals 29
3.6.1 Initial Justification Based Research 29
3.6.2 Case Study: Unfiltered Apps – What are the risks? 29
3.6.3 App Safety System 30
3.6.4 App research 30
3.6.5 Blog 30
4.0: Scope and Reasoning 31
4.1 Initial Research 31
4.2 Case Study 31
4.3 Researching App Terms & Conditions 32
4.4 Researching App Features & Settings 32
4.5 Blog 34
5.0 Deliverables 35
6.0 Feasibility Study 36
6.1 Hotline.ie 40
6.2 BeSafeOnline 44
6.3 Webwise.ie 45
6.4 WhatsApp as featured by Webwise.ie 50
6.5 YouTube as featured by Webwise.ie 54
6.6 ISPCC – Childline 57
6.7 NPC Primary 58
6.8 CyberSafeIreland 59

6.9 Feasibility Study Determination 61
7.0: Proposal 62
8.0 Literature Review – Unfiltered Access to Apps – What are the risks? 63
8.1 CyberSafeIreland's 2017/18 Annual Reports 63
8.2: Custom Child App & Platform Use Survey 69
8.3 Custom Child App & Platform Use Survey Results 74
8.4 Google Play Store / Apple Store 84
8.5 App Selection 89
8.6 Risk Relating to Unfiltered Online Access 91
8.6.1 Predators & Grooming 91
8.6.1.1 Case 1 91
8.6.1.2 Case 2 93
8.7 Risks of Unfiltered Access to Snapchat 94
8.8 Risks of Unfiltered Access to Instagram 97
8.8.1 Data Breaches 98
8.8.2 Instagram Inappropriate Content 99
8.9 Risks of Unfiltered Access to WhatsApp 101
8.10 YouTube / Google Family-Link / YouTube Kids Case Study 103
9.0 App Safety Rating System Breakdown 105
10.0 Brief explanation of VPN's 107
11.0 Primary Research Outcomes 108
11.1 Snapchat 108
11.1.1 Snapchat Terms & Conditions: 108
11.1.2 Snapchat Features 112
11.1.3 Snapchats Personal Security Optimization Options 113
11.1.4 Snapchat Settings 114
11.1.5 Blocking Users 120
11.1.6 Snapchat Best Practice Settings Guide 122
11.1.7 Snapchat App Safety Rating 122
11.1.8 Reflections on Snapchat 123
11.2 Instagram 123
11.2.1 Instagram Terms & Conditions 123
11.2.2 Instagram Features 131
11.2.3 Instagram's Personal Security Optimization Options 131
11.2.4 Instagram Settings 131

11.2.5 Instagram Best Practice Settings Guide 173
11.2.6 Instagram App Safety Rating 174
11.2.7 Reflections on Instagram 175
11.3 WhatsApp 176
11.3.1 Introduction to WhatsApp 176
11.3.2 Fees & Charges 176
11.3.3 WhatsApp Terms & conditions 177
11.3.4 WhatsApp Features 182
11.3.5 Money Transfer via WhatsApp Payment 182
11.3.6 How Safe is WhatsApp? 183
11.3.7 WhatsApp & Facebook Family Data Breaches 183
11.3.8 WhatsApp's Personal Security Optimization Options 184
11.3.9 WhatsApp Settings 185
11.3.10 WhatsApp Best Practice Settings Guide 203
11.3.11 WhatsApp App Safety Rating 204
11.3.12 Reflections on WhatsApp 205
11.4 YouTube / Google Family-Link / YouTube Kids 206
11.4.1 YouTube 206
11.4.1.1 YouTube and Google's Terms & Conditions 206
11.4.1.2 Age Limits 207
11.4.1.3 Privacy Policy & Data Sharing 207
11.4.1.4 Data Processing Terms 208
11.4.1.5 Abuse and Behaviour 209
11.4.1.6 Security 210
11.4.1.7 The Nature of Data Collected 210
11.4.1.8 YouTube Features 211
11.4.1.9 YouTube's Personal Security Optimization Options 214
11.4.1.10 YouTube Settings 214
11.4.1.11 Securing the Google Account 217
11.4.1.12 YouTube Best Practice Settings Guide 228
12.4.1.12 YouTube App Safety Rating 228
11.4.1.13 Reflections on YouTube 229
11.4.2 Google Family-Link 229
11.4.2.1 Google Family-Link Features 230
11.4.2.2 Google Family-Link's Personal Security Optimization Options 230

11.4.2.3 Google Family-Link Setup 231
11.4.2.4 Google Family-Link Settings 255
11.4.2.5 Google Family-Link Best Practice Settings Guide 292
11.4.2.6 Google Family-Link App Safety Rating 293
11.4.2.6 Reflections on Family-Link: 293
11.4.3 YouTube Kids 294
11.4.3.1 YouTube Kids without family link 296
11.4.3.2 YouTube with Family Link 298
11.4.3.3 YouTube kids features without Family Link 301
11.4.3.4 YouTube Kids features with Family Link 307
11.4.3.5 YouTube Kids' Personal Security Optimization Options 309
11.4.3.6 YouTube Kids Settings 310
11.4.3.7 YouTube Kids Best Practice Settings Guide 314
11.4.3.8 YouTube Kids App Safety Rating 315
11.4.3.8 Reflections on YouTube Kids 315
12.0 Website 317
12.1 Goal of Website 317
12.2 Design Phase 317
12.3 Implementation 318
12.4 Design 319
12.4 Use Test Case for Our Website 322
13.0 Conclusions 326
13.1 Future Work 332
13.1.1 Test Case Demonstration of App 332
14.0 Appendix 344
15.0 Glossary 358
16.0 References 360

1.0 Table of Tables

Table 1 Results of email type study carried out by the Cisco Talos Group over a one month period **(Cisco , 2019).** 21
Table 2 Ownership of smartphones by age. 2018 CyberSafeIreland annual report **(CyberSafeIreland 2018, page 17)**. 63
Table 3 Use of Social Media & Messaging Apps among children aged 8 -13. 2018 CyberSafeIreland annual report **(Ibid) (page 18 2018).** 64
Table 4 Chart of children talking to strangers online listed by age. 2018 CyberSafeIreland annual report **(Ibid) (page 20 2018).** 65
Table 5 Chart of frequency of online contact with strangers among children surveyed. 2018 CyberSafeIreland annual report **(Ibid) (page 21 2018).** 65
Table 6 Frequency of yearly on-line related incidents faced by teachers regarding their pupils. 2018 CyberSafeIreland annual report **(Ibid) (page 25 2018).** 66
Table 7 Survey of parent's ability to implement CyberSafeIreland's recommendations from their information sessions. 2018 CyberSafeIreland annual report **(Ibid) (Page 25 2018).** 67
Table 8 Survey of parents whose children had spoken them about online safety by age. 2018 CyberSafeIreland annual report **(Ibid) (page 24 2018).** 67
Table 9 Instances of young users of YouTube posting videos, by age. 2018 CyberSafeIreland annual report **(Ibid) (page 22 2018).** 68
Table 10 Instances of young users of YouTube appearing in videos, by age. 2018 CyberSafeIreland annual report **(Ibid) (page 22 2018).** 69
Table 11 Results of question pertaining to platform use, conducted February 2019. 74
Table 12 Results pertaining to the age of the child in question, conducted February 2019. 75
Table 13 Results pertaining to the Apps the child uses, conducted February 2019. 76
Table 14 Results pertaining to parents or supervisors providing online access to children who don't have their own device, conducted February 2019. 77
Table 15 Results pertaining to concerns about online safety, conducted February 2019. 78
Table 16 Results pertaining to how parents or supervisors understand security features on selected Apps, conducted February 2019. 79
Table 17 Results from Google Play store, Ireland, Social App Type **(SimilarWeb 2019) [Accessed March 2019].** 85
Table 18 Results from the Apple store, Ireland, Social App Type **(Ibid 2019) [Accessed March 2019]**. 86
Table 19 Results from Android store, Ireland, Entertainment App Type **(SimilarWeb 2019) [Accessed March 2019]**. 87
Table 20 Result from the Apple Store, Ireland, Entertainment App Type **(SimilarWeb 2019) [Accessed March 2019]**. 88
Table 21 Results of Child focused App & Platform use Survey conducted via Survey monkey. 177

2.0 Table of Figures

Figure 1 Hotline initiate as documented on The Department of Justice & Equalities website, **(Department of Justice & Equality 2019) [Accessed March 2019]** 36
Figure 2 Action plan establish by The Department of Justice & Equalities website, **(Ibid) [Accessed March 2019]** 36
Figure 3 Progress report published by The Department of Justice & Equality **(Department of Justice & Equality – Progress Report on Action Plan for Online Safety 2018) [Accessed March 2019]**. 37
Figure 4 The gov.ie portal link to the BeSafeOnline awareness campaign as documented on The Department of Justice & Equalities website, **(Department of Justice & Equality 2019) [Accessed March 2019]** 38
Figure 5 The EU Safer Ireland Initiative resources as documented on The Department of Justice & Equalities website, **(Department of Justice & Equality 2019) [Accessed March 2019]** 39
Figure 6 Internet Safety Day, as documented on The Department of Justice & Equalities website, **(Department of Justice & Equality 2019) [Accessed March 2019]** 39
Figure 7 Information & services n offered by Hotline.ie related to Online secirity and risk reduction. **(Hotline.ie – Internet Safety 2019)[Accessed March 2019]** 40
Figure 8 Hotline.ie report content feature. **(Hotline.ie – Make a Report 2019)[Accessed March 2019]** 41
Figure 9 General online safety tips offered by Hotline.ie **(Hotline.ie – Safety Tips 2019)[Accessed March 2019]** 42
Figure 10 Hotline.ie filtering services advice and recommendations page **(Hotline.ie – Filtering Software 2019)[Accessed March 2019].** 43
Figure 11 Sample of links offered by the Gov.ie portal service BeSafeOnline **(Gov.ie 2019) [Accessed March]**. 44
Figure 12 Webwise.ie homepage **(Webwise.ie 2019) [Accessed March 2019].** 45
Figure 13 Webwise.ie homepage, get Resources link **(Webwise.ie 2019) [Accessed March 2019].** 46
Figure 14 Tips and trending content offered by Webwise.ie **(Webwise.ie 2019) [Accessed March 2019].** 46
Figure 15 Webwise.ie homepage, Apps explained section **(Webwise.ie 2019) [Accessed March 2019].** 47
Figure 16 Webwise.ie homepage teachers resource information and training links **(Ibid) [Accessed March 2019].** 47
Figure 17 Webwise.ie homepage parents resource chat and advice links **(Ibid) [Accessed March 2019].** 48
Figure 18 14 Webwise.ie homepage Teachers video media links **(Ibid) [Accessed March 2019].** 48
Figure 19 Breakdown of WhatsApp App by Webwise.ie **(Webwise.ie 2019) [Accessed March 2019].** .. 50
Figure 20 Webwise featuring WhatsApp features warning of possible costs relating to data roaming **(Ibid) [Accessed March 2019].** 51
Figure 21 Webwise Draws attention to the GPRS tracking feature contained within WhatsApp **(Ibid) [Accessed March 2019].** 52
Figure 22 Webwise docments enabling locations sharing on an IOS device, and editing feature **(Ibid) [Accessed March 2019].** 52
Figure 23 Webwise.ie coverage of age-based account visibility related settings in WhatsApp **(Ibid) [Accessed March 2019].** 53
Figure 24 Webwise.ie explains what YouTube is, Apps explained section **(Webwise.ie 2019) [Accessed March 2019].** 54
Figure 25 Webwise.ie covers the features of YouTube in a very minimalist fashion **(Ibid) [Accessed March 2019].** 54
Figure 26 Webwise.ie covers YouTubes age restriction **(Ibid) [Accessed March 2019].** 55

Figure 27 Webwise.ie covers the risks associated with inappropriate content being displayed within YouTube **(Ibid) [Accessed March 2019].** 55
Figure 28 Webwise.ie covers the risks of cyberbullying associated with YouTube use **(Ibid) [Accessed March 2019].** 56
Figure 29 Webwise.ie covers privacy settings and parental controls **(Ibid) [Accessed March 2019].** 56
Figure 30 Webwise.ie draws attention to the ability to disable comments and YouTube's Safety Mode **(Ibid) [Accessed March 2019].** 57
Figure 31 The NPC Primary's online video catalogue of guides related to internet safety **(WWW.npc.IE) [Accessed March 2019].** 58
Figure 32 CyberSafeIreland presents links to settings to filter explicit content via Google and YouTube **(Parental Controls) [Accessed March 2019].** 59
Figure 33 CyberSafeIreland's link takes us directly to YouTubes Support site **(YouTube Help Centre) [Accessed March 2019].** 60
Figure 34 Question 1 our survey relating to platform use, conducted February 2019. 70
Figure 35 Question 2 our survey in relation to age, conducted February 2019. 70
Figure 36 Question 3 of our survey relating to specific App use, conducted February 2019. 71
Figure 37 Question 4 of our survey in relation to online access, be it from personal or parent/supervisor accounts, conducted February 2019. 72
Figure 38 Question 5 aims at the level of awareness of parents regarding the risks of online access, conducted February 2019. 72
Figure 39 Question 6 is designed to discover the necessity for our need for our planned product (our blog), conducted February 2019. 73
Figure 40 Question 7 allows for optional feedback from survey participants relating to security, conducted February 2019. 73
Figure 41 number of survey respondents. 74
Figure 42 Finally, an Optional text box for participants to provide security related feedback for Apps 79
Figure 43 Optional Response 1 from our custom Child App & Platform Use Survey, conducted February 2019. 80
Figure 44 Optional Response 2 from our custom Child App & Platform Use Survey, conducted February 2019. 80
Figure 45 Option Response 3 from our custom Child App & Platform Use Survey, conducted February 2019. 80
Figure 46 Optional Response 4 from our custom Child App & Platform Use Survey, conducted February 2019. 81
Figure 47 Optional Response 5 from our custom Child App & Platform Use Survey, conducted February 2019. 81
Figure 48 Optional Response 6 from our custom Child App & Platform Use Survey, conducted February 2019. 81
Figure 49 Optional Response 7 from our custom Child App & Platform Use Survey, conducted February 2019. 82
Figure 50 Optional Response 8 from our custom Child App & Platform Use Survey, conducted February 2019. 82
Figure 51 Optional Response 9 from our custom Child App & Platform Use Survey, conducted February 2019. 82
Figure 52 Optional Response 10 from our custom Child App & Platform Use Survey, conducted February 2019. 83

Figure 53 Optional Response 11 from our custom Child App & Platform Use Survey, conducted February 2019. 83
Figure 54 Optional Response 12 from our custom Child App & Platform Use Survey, conducted February 2019. 83
Figure 55 Optional Response 13 from our custom Child App & Platform Use Survey, conducted February 2019. 84
Figure 56 Chart from the 2017 Hotline.ie Annual Report **(Hotline.ie) [Accessed March 2019]** 92
Figure 57 An example of inappropriate content for young children. 95
Figure 58 Statistics on percentage of active users on Instagram, split by age range and gender **(Statistica.com 2018) [Accessed Feb 2019].** 97
Figure 59 A sponsored photo from Kylie Jenner's Instagram page **(Jenner k. 2018) [Accessed March 2019].** 98
Figure 60 An example of potentially age-inappropriate material from Instagram **(AdultCouple 2019) [Accessed on 20th March 2019].** 99
Figure 61 Babepedia Instagram profile with a link to their pornagraphic website. 100
Figure 62 An example of three fake celebrity accounts, one being a parody account **(Computer Hope 2018) [Accessed Feb 2019].** 100
Figure 63 Kim Kardashians Instagram post about Momo **(Lewis S. 2019) [Accessed Feb 2019].** 102
Figure 64 Here we see an example of some videos that fall into the Elsa-gate category of videos. 103
Figure 65 Our App Rating Graphic. 106
Figure 66 Picture of the SnapMap Feature of Snapchat. 113
Figure 67 How to get to Snapchat Settings 114
Figure 68 Changing who can Contact you on Snapchat 115
Figure 69 Above you can set who can send you Snaps. 116
Figure 70 Accessing the Story settings. 117
Figure 71 Control who can see your story. 117
Figure 72 Managing Who can see your Location in Snapchat. 118
Figure 73 Selecting specific friends who can see your location in Snapchat. 119
Figure 74 Managing the Quick Add Function in Snapchat 120
Figure 75 Managing Users in Snapchat 121
Figure 76 Managing Users in Snapchat 121
Figure 77 For Breakdown of Points System, please see: 10.0 App Safety Rating System. 122
Figure 78 Private account toggle switch. 132
Figure 79 The button where Instagram TV can be accessed. 133
Figure 80 A user being tagged in a photo. 134
Figure 81 Deletion of a comment. 135
Figure 82 A follow request. 136
Figure 83 Here, the user has received a message request from another user, which will allow the unknown contact to communicate with the user. 137
Figure 84 Here, we see the user about to unsend a message that was previously sent to another user. 138
Figure 85 Here, we see the user about to block another user. 139
Figure 86 Here we see were the story option can be accessed. 140
Figure 87 An example of a generic comment on a live stream. 141
Figure 88 Story Controls. 142
Figure 89 From left to right we can see the sequence of the reporting process 143
Figure 90 Here we can see a user being unfollowed. 144
Figure 91 Instagram requesting the permission of a parent or guardian in the relation of showing ads 145

Figure 92 The act of hiding or reporting an advertisement. 146
Figure 93 The user in the process of archiving content. 147
Figure 94 The process of retrieving achieved content. 148
Figure 95 A user about to retrieve their own content. 149
Figure 96 All the folders and files which are sent to the user because of retrieving data. 150
Figure 97 This section allows for a user to view all their data that Instagram stores. 151
Figure 98 From left to right, accessing the privacy and settings option. 152
Figure 99 Implantation of private mode in the Account Privacy section. 153
Figure 100 Here we see the option to toggle automatic adding of photos you are tagged in and the ability to hide said photos. 154
Figure 101 Accessing the story settings on the Instagram app. 155
Figure 102 The toggle to automatically share your story to Facebook. 156
Figure 103 Here we see the option to choose can reply to stories. 157
Figure 104 Here we see the option to hide your story from people. 158
Figure 105 Here we see the option to add users to a close friends list. 159
Figure 106 Here, we see the comment control settings on the left and the hide offensive comments filter toggle on the right. 160
Figure 107 Here we see the feature which allows the unblocking of blocked users. 161
Figure 108 Here we see the activity status toggle which, when activated, will allow users to see your activity statues. toggle off to be invisible. 162
Figure 109 Here we see the section for changing the password to the Account 163
Figure 110 Here we see the option menu for the Two Step Authentication menu. 164
Figure 111 Here we see the recovery codes that are available after setting up a two-factor authentication. 165
Figure 112 Here we see how a user can access the payment option on the App. 166
Figure 113 Here we see the setting to add a payment option to your account. 167
Figure 114 Here we see the option to add a Security Pin to the account to secure the payment option. 168
Figure 115 Here we see the option to link an account to your Instagram account 169
Figure 116 Here we see the toggle to allow syncing of contacts to an account. 170
Figure 117 Here we see the process in which a user can add or remove a Geolocation tag. 171
Figure 118 Here we see the options available when editing the user. 172
Figure 119 Here we see the process to remove tagging on a photo on another user's photo. 173
Figure 120 For Breakdown of Points System, please see: 10.0 App Safety Rating System. 174
Figure 121 Select the three dots to enter settings menu. 185
Figure 122 Now Select settings. 186
Figure 123 Here we are at the main settings menu. 187
Figure 124 Here we see the 'Last Seen', 'Profile Picture and 'About' settings options adjusted to reduce online footprint. 188
Figure 125 Here we see the status sharing options displayed, with sharing to all excluding one contact shown first, followed by sharing restricted to one contact. First, 'Dad; is restricted from seeing the status, then status is only shown to 'Dad'. 189
Figure 126 As seen above, GPRS based location services are deactivated on my android device, therefore WhatsApp cannot collect or display location-based data. 190
Figure 127 Here we see the contact blocking options. 191
Figure 128 Here we see the toggle option for 'Read Recipients'. 192
Figure 129 Here we see the security options selected and security notifications enabled. 193

Figure 130 Here we see the setting up of Two Step Verification. First, we select the option via the main account settings menu. Next, we select enable. We are then asked to enter and reconfirm our pin number. 194
Figure 131 Finally, we enter and reconfirm an E-mail for resetting our pin, and we receive a setup confirmation message. Should we wish to reset any details we simply renter the Two Step Verification menu. 195
Figure 132 Here we see the Request Account Info option highlighted. 196
Figure 133 Here we see the in chat 'Export Chat' options highlighted. 197
Figure 134 Here we see the chat settings being select from the main settings menu, followed by the chat backup option being selected. 198
Figure 135 Here we see the 'Google Drive' settings being selected, and the chat backup frequency being set to 'Never' 199
Figure 136 Here we have selected the content we intend to delete, by tapping the desired content. Next, we select the delete icon from the top of the chat. 200
Figure 137 Here we see the available options for deleting the content from within a chat. 201
Figure 138 Here we see the chat options being selected via the 3 dots, followed by the more option setting. 202
Figure 139 Here we see the 'Report option being selected. 203
Figure 140 For Breakdown of Points System, please see: 10.0 App Safety 204
Figure 141 The home page of YouTube. 211
Figure 142 On the left we see the liking feature and on the right, we see the Library tab. 212
Figure 143 My Channel Page in the Library Tab 213
Figure 144 Locating the Settings. 214
Figure 145 Locating Restricted Mode in General Settings 215
Figure 146 Blocking a User on YouTube. 216
Figure 147 Home page of David's Google Account 217
Figure 148 Data & Protection Tab in David's Google Account. 219
Figure 149 Viewing the Security Issues on David's Google Account. 220
Figure 150 Viewing the About Me page of David's Google Account 221
Figure 151 About Me page for David's Google Account 222
Figure 152 Security Tab of David's Google Account 223
Figure 153 WinRAR Extraction of the Data Downloaded 224
Figure 154 How to Download a User's Data. 225
Figure 155 Making Plans for a Google Account 226
Figure 156 Managing a User's Shared Endorsements 227
Figure 157 For Breakdown of Points System, please see: 10.0 App Safety 228
Figure 158 Here we select the create account option. 231
Figure 159 Now we select "For My Child". 232
Figure 160 Here is a brief overview of the options available for parents in supervising your child's account, simply select "yes, continue" 232
Figure 161 Enter your number to receive your verification code. 233
Figure 162 Now enter your child's date of birth. 233
Figure 163 Chose an appropriate email account for your child. 234
Figure 164 Enter an appropriate password, following the security recommendations above. 235
Figure 165 Now you must sign in as a parent on your own Google account. 235
Figure 166 Enter your Google accounts password. 236
Figure 167 Enter two step verification code if required. 236

Figure 168 Overview of some of the options available. 237
Figure 169 Select “I Agree” to add your child’s account to your family group. 238
Figure 170 This is acknowledgement of the data protection policies and sharing employed by google. By accepting you are consenting to have Google manage your child’s data and account. 239
Figure 171 Here google outline the function available which a parent may wish to secure via Family-Link, such as browser searching, emails, chats, video and voice calls etc. 239
Figure 172 Once again, a slightly more verbose overview of the functions available in Family-Link. ... 240
Figure 173 This simply outlines that the Family-Link App is required to access all the functions offered by Family-Link. 240
Figure 174 This section outlines the purchasing and approval polices by Google under Family-Link. By default, the parent must approve all purchases. 241
Figure 175 Privacy information continued, as well beginning to document data collection policy. 241
Figure 176 Information regarding the collection of data from a child’s online activity. 242
Figure 177 Information regarding the collection of data from your child’s in App activity, voice and video data and location data. 242
Figure 178 Information regarding how data is collected, and on what kinds of data your child can share both with and without consent. 243
Figure 179 Information regarding the visibility of your child’s account regardless of how restrictive your settings are. 244
Figure 180 Information regarding the sharing of data between YouTube and its partners. 244
Figure 181 Information regarding who can access your child’s personal information. 245
Figure 182 Information regarding the deleting of your child’s account and how it will stop the collection of data. 245
Figure 183 Once your child turns 13, because they can technically manage their own account from this point on. The child can take over the account without the parent’s approval at this point despite the digital age of consent in Ireland. 245
Figure 184 Contact information for Google US, however Google is managed in Ireland by Googled Ireland LLC. 246
Figure 185 Finally, the parent must accept the above terms & conditions, as previously covered. 246
Figure 186 Here we begin to restrict the child’s access to unauthorized services. 247
Figure 187 Select the age group of the content most appropriate for your child. 248
Figure 188 Select the most age appropriate movies settings. 248
Figure 189 Select an appropriate age group for the movies your child will have access to. 249
Figure 190 Here can see protections automatically applied for Google Books. 249
Figure 191 Again, here can see protections automatically applied for Google Music. 250
Figure 192 Here we can see filters are applied for Google Chrome browser content and search content. 250
Figure 193 Here, we have increased the restrictions on google Chrome filters. 251
Figure 194 Here we see the safe search filters are automatically applied to Google Chrome. 251
Figure 195 Now we can finally install the Family-Link App. 252
Figure 196 Here we are, installing the Family-Link App on our ‘Test’ child’s tablet. 252
Figure 197 The App has scanned our child’s tablet and presented us with a list of Apps to review and decide which would like to keep or uninstall. 253
Figure 198 Here we have deactivated google bac-ups, and location data options. 253
Figure 199 Lastly, we disable usage data collection. Updates cannot be disabled. 254
Figure 200 Here we see Family-Link set up on our “Test” child’s Tablet device. 254

Figure 201 Here, we can see the Parent managing the “test” child’s account from our group members Google account via his phone. 255
Figure 202 Here we have the main menu for Family-Link displaying all the Child accounts my account is currently managing. 256
Figure 203 Here we see the test child accounts we added to our parent account. 257
Figure 204 Here we can invite family members, assign supervisor roles and manage parental privileges as needed. 258
Figure 205 Here we can select the family group menu. 258
Figure 206 Select this menu to approve or deny requests. 259
Figure 207 Here we see an approval request message has been sent from the child account. 260
Figure 208 Here we can approve or deny the request simply be selecting the appropriate option. 260
Figure 209 Here we see the request is denied on the child’s device. 261
Figure 210 Here we can see the parental code menu option displayed. 262
Figure 211 Here we see the parental access code. This code changes regularly as you can see by the timer above. 263
Figure 212 Here, we select the notification management settings. 264
Figure 213 Here we see the available categories of notifications. 265
Figure 214 Here we can manage the notifications related to new Apps. 266
Figure 215 Here we can see the available options for Website notifications. 266
Figure 216 Here we can see the options available for Activity notifications. 267
Figure 217 Here we see the tips and help/feedback menus. 268
Figure 218 Here we see a sample of the tips displayed in the tip’s menu. We strongly recommend parents examine these tips. 269
Figure 219 Here we see some of the help and feedbacks options displayed. Again, we strongly recommend parents examine this section in depth. 269
Figure 220 Here we see the options mentioned previously which give us access to other options pertaining to account management. 270
Figure 221 Here see, once again the family group options. Please note the three dots which contain the ‘Delete family Group” option. 271
Figure 222 Here we see the delete family group option displayed, use caution as this will also remove your child’s account and prevent you from managing it. 271
Figure 223 Here we see the + add child account option. 272
Figure 224 Here we can see that we can now add a new child account. 272
Figure 225 Here we select the account we wish to manage, in this case the “Test” account. 273
Figure 226 Here we are, in the Test account management menu screen. 274
Figure 227 Select account info to alter the account information for your child. 274
Figure 228 Here we can access and alter the account details of our child’s account. Including changing the password and deleting the account should we desire. 275
Figure 229 Here, we can manage the profile picture for our child’s account. 276
Figure 230 We can now add a profile picture, however, as this is a child’s account we have elected not to use one due to the risks associated with predators. 276
Figure 231 Here we can enter the parental settings management menu. 277
Figure 232 As you can see, we can alter the settings selected during install which govern the rules under which out child’s device operates. 278
Figure 233 Further options are available within this menu by selecting “more” as seen above. 278
Figure 234 First, we can alter the settings relating to approval requests. 279

Figure 235 As you can see we elected to retain our strict settings here as this affords the highest degree of security and peace of mind for parents. 279
Figure 236 Here we have elected to increase the age limit on Apps, so that out child may access games more appropriate to his/her age level. 280
Figure 237 Again, we increase the age limit allowing access to more age appropriate movies via Google Movies. 280
Figure 238 Here we can manage third-part Apps, add our child's account to other devices and managing the Google assistant's ability to understand and recognize out child's voice. We strongly recommend disabling access to third-party Apps. 281
Figure 239 Here you can see the Google assistant related settings. We recommend leaving these off as they only serve to provide Google with data to collect. 282
Figure 240 As you can see here, enabling location tracking is as simple as selecting setup. 282
Figure 241 Here we see out child's device location! Or do we? See below for an explanation. 283
Figure 242 Select more to view the options pertaining to Apps and select the App whose settings you wish to alter. 284
Figure 243 Here we see that we are presented with menus by time and date. We have selected 'yesterday'. And will now select YouTube Kids. 284
Figure 244 Here we can see YouTube Kids is selected. From here we can remove the Apps allow status and view the Apps permissions 285
Figure 245 Here we can view the permissions the App has internally on our child's device and manage these settings. 285
Figure 246 Here can set up the screen time locks as desired. 286
Figure 247 Here we can set up our daytime screen locks. 287
Figure 248 Here we can set up our night time screen locks. 287
Figure 249 Here we can see secondary access provided to App settings via the child account management menu. 288
Figure 250 Here we can access some useful data relating to setting on the child's device, as well as playing a test sound to ensure the Accounts are correctly synced. 289
Figure 251 Here we see the test sound playing on my child's device. 289
Figure 252 Here see device related settings on the child's device. 290
Figure 253 Here, a parent can gain access to Googles privacy terms & conditions as well as trouble shooting steps. 291
Figure 254 Here we see the menu from the perspective of the child. As you can see it is extremely limited. 291
Figure 255 Here, we see the profile selection page on YouTube Kids 295
Figure 256 The Welcoming page of YouTube kids, informing a child to get a parent's permission to unlock the App. 296
Figure 257 Here we see the application asking for the parents age 296
Figure 258 Here we see the application asking for a simple mathematical question 297
Figure 259 Here, we see the application providing information on how to block and report videos on the application. 297
Figure 260 The implementation of a VPN 299
Figure 261 Choosing the age range of your child. 300
Figure 262 YouTube Kids maths-based challenge code. 301
Figure 263 YouTube Kids parental options. 302
Figure 264 YouTube Kids settings menu. 302
Figure 265 Entering your parental password to access restricted settings 303

Figure 266 Further parental options. 304
Figure 267 Content selection from channels based on themes. 305
Figure 268 Quality of life access to previous settings, no longer password protected not that your password has been entered. 305
Figure 269 Manual blocking of content. 306
Figure 270 Blocking content by channel or creator. 306
Figure 271 Unblocking videos. 307
Figure 272 Managing YouTube Kids settings via Google Family-Link. 308
Figure 273 Privacy settings remain accessible on the YouTube Kids App presenting a potential issue. 309
Figure 274 Accessing settings without Family-Link installed. 310
Figure 275 Restricting the search function. 311
Figure 276 How to restrict the search function of YouTube Kids when it is combined with Google Family-Link. 312
Figure 277 Creating a secret code for your child. 313
Figure 278 For Breakdown of Points System, please see: 10.0 App Safety 315
Figure 279 The first feedback question in our website use test case survey. 322
Figure 280 The second feedback question from our website use test case survey. 323
Figure 281 The third feedback question from our website use test case survey. 323
Figure 282 The fourth feedback question from our website use test case survey. 323
Figure 283 The fifth feedback question from our websites use test case survey. 324
Figure 284 The sixth feedback question from our website use test case survey. 324
Figure 285 The seventh feedback question from our website use test case survey. 324
Figure 286 The eight-feedback question from our website use test case survey. 324
Figure 287 The ninth feedback question from our website use test case survey. 325
Figure 288 Unfiltered access to inappropriate content 334
Figure 289 We see a different set of search results. 335
Figure 290 Here we see comments disabled via restricted mode for our second test account 336
Figure 291 Here we see the public video posted to the second test account with restricted mode enabled, but a comment may still be placed. 337
Figure 292 Here, we see a friend request sent via Facebook to our second test account from the malicious user account. 338
Figure 293 Here we see the blocked malicious user has sent a further request and our child has been warned that accepting this link will remove the block. 338
Figure 294 Here we can see the default arrangement of google data gathering settings. These we switch to off. 339
Figure 295 Here, we see googles shared endorsements setting is on be default. This was also tuned off. 339
Figure 296 Parental options adjusted as per our guide. 341
Figure 297 Parental options adjusted as per our guide. 341
Figure 298 Here we see fully positive feedback regarding the usability of our navigation bar. 344
Figure 299 Here we see the feedback regarding the accessibility of our content. 345
Figure 300 Question 3 glitched and produced invalid results. 346
Figure 301 Here we see the results of question 4, aimed at gathering feedback on the overall presentability of the site. 347
Figure 302 Here we see the interesting results we received from question 5 348
Figure 303 This question was designed to gather feedback on the usefulness of our blog function. Most users found the feature useful. 349

Figure 304 Question 7 highlights our feedback regarding level of difficulty in implementing our guides. 350
Figure 305 Question 8 is simply designed to determine if users feel they are anonymous enough while using our service. 351
Figure 306 General overview of primary analytical data pertaining to www.safeappuse.ie website after two weeks live..... 353
Figure 307 Pageviews per page on www.safeappuse.ie after two-week period 354
Figure 308 here we see top 20 Client ID session data showing returning users 355
Figure 309 Here we see users who come to our website based on operating system 355
Figure 310 Acquisition statistics for www.safeappuse.ie in two weeks 356
Figure 311 Here we can see the users who came to our website by location 357

3.0 Introduction

3.1 Motivation

Security in the digital age can be a complicated minefield for even the most highly educated and trained professionals, let alone the average person trying to navigate their way through the many millions of operating systems, devices, Apps, and other third-party software systems on the market. And that is assuming that the average person is even conscious of the potential traps, flaws and pit-falls they may encounter and takes steps to avoid them, which of course, those of us who study this field will know is simply not true. The average person expects the developers to secure the software and assume they will have done this. This tends to provide a false sense of security as mobile platforms for example, tend to carry inherent risks and security tends to be minimal **(Symantec, 2014)**. To develop a habit of leaving your security in the hands of others and simply assume they have secured your data, identity or device is obviously a bad habit to develop, but it is even more dangerous when children are involved.

A child may see the world differently to an adult particularly if the parent adopts a more permissive parenting style **(Sahara Byrne et al , 2014)** and being possessed with the kind of innocence that is stripped from an adult as we grow, may be unaware that there are people who exist in the world that may want to hurt them; be it for profit or for their own amusement however twisted it might be. As such, a child's security precautions may be determined by the guiding hands of an adult who has made some effort to establish guidelines regarding a child's online activity but who may also lack adequate knowledge of the risks that exist. Or, the child's safety has been left to be determined by the program they are using, or they are simply very lacking bordering on non-existent. This is not to suggest that no parents are making informed decisions, but this is not an easy process to get right and information can be hard to come by. While it is our curiosity as children that drives us to learn, this curiosity unguided and unfiltered and supervised can lead us to danger and this is no less true in the digital age.

Along-side this risk to children, comes the risks associated with adults being unaware of the dangers that exist. With our modern hectic lifestyles, it is perfectly understandable that a parent may hand a device to a child hoping for a moments distraction to take a breather, completely unaware that some online users may be seeking to take advantage of their lack of awareness coupled with the natural innate curiosity of their child to seek to manipulate them. Some of these malicious users may be predators, some may simple be mentally damaged individuals and some may be criminals seeking a financial gain.

There is of course a further risk factor, less dangerous perhaps, but no less unwanted by users. As well as the risks associated with the modern digital age mentioned above, there is also the risks associated with the monetization of data. Each of us, both adult and child, has an online footprint. And that footprint leaves a data trail that marketers and manufacturers of products can use to target consumers and predict trends. Worse still, users' data can be used maliciously to manipulate their decision-making processes. Dis-information and disingenuous stories are becoming very pervasive across social media platforms. This can have a very detrimental effect on society and more importantly can have a very negative impact on children. The monetization of data is fast becoming one of the world's biggest online industries that drives the modern consumer market. To avoid unwanted consumer solicitations, both legitimate and illegitimate spam and most importantly to reduce the targeting of children by marketing companies, it is best to attempt to reduce the on-line footprint, by where ever possible, reducing the visibility of your data via your profiles and data sharing options.

With Your data being monetized, you are effectively monetized. Your online habits, uses, sites you visit and purchases you make reveal a lot about you and your decision-making processes. This makes you a prime target for spam, phishing and any site that may be able to collect your meta-data to sell them to marketing agencies. To put this into some context, as illustrated by **(Shneyder L., 2018)**, experts at cisco using their security team Talos, set up a trap server for the purposes of documenting the type of email traffic trapped. It was estimated that over a one-month period, of the almost 45 billion emails screened through this server, just over 85% of the emails were considering to spam or illegitimate emails. And this is just one form of information phishing.

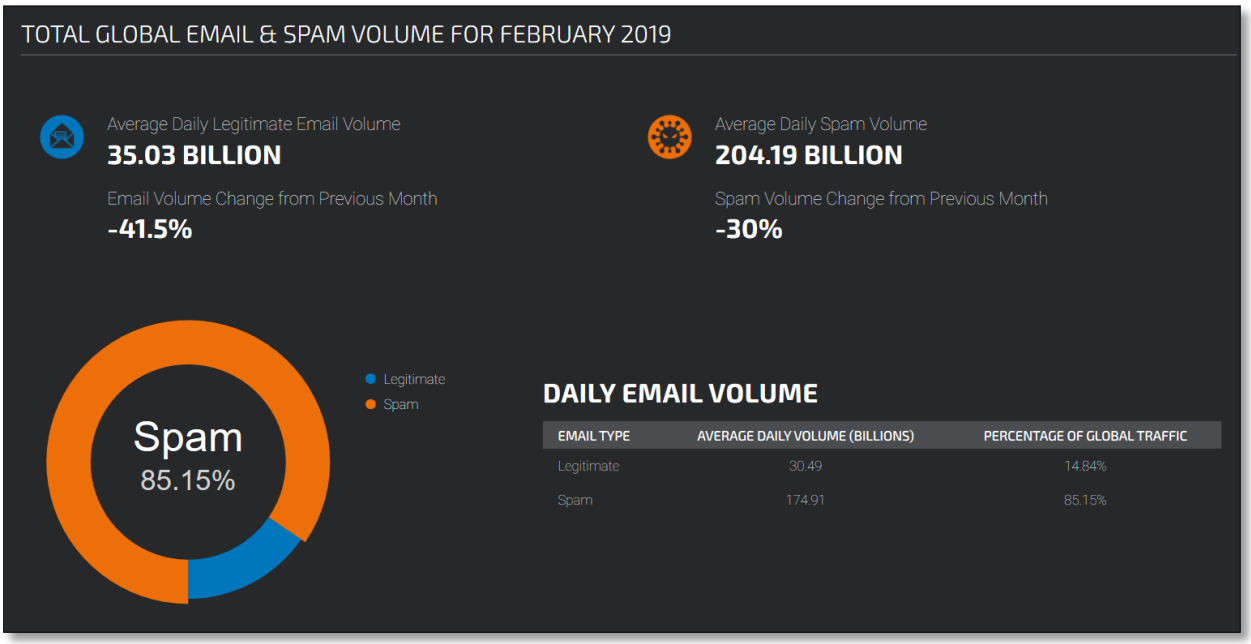


Table 1 Results of email type study carried out by the Cisco Talos Group over a one month period ***(Cisco , 2019).***

So, how exactly do we remedy this and reduce the potential risks? Well, the options vary from App to App, operating system to operating system and software to software, not to mention websites. And where exactly does one go to learn the skills and obtain the knowledge needed to best know how to adjust these settings or which security Apps to employ to best protect yourself, your identity and most importantly those your child?

These are precisely the questions our group aims to answer. We will conduct research to establish the most commonly used Apps among children in Ireland. Taking platform into consideration, though this is less of a concern as technology develops and Apps become more and more progressively cross-platform. We shall use pre-existing pertinent research as well as conducting our own survey to determine which Apps to study.

Once we have selected our appropriate Apps, we shall conduct an overall case study of the risks and dangers associated with App use among children. Having conducted our case studies we shall develop a simple App safety rating system to determine which of the Apps we investigate are safe for use by children. Next, we will perform in depth analysis of the features of each App. Finally, we will delve into the settings to establish the most secure settings to select, to better reduce your or your child's online footprint and visibility.

Once we have investigated each App and established our recommendations for increasing security when using each App, we shall then develop a Web based platform to present this information in a user-friendly format. This is the goal of our program. To produce a useable practical blog based of our research which will allow parents to make informed decisions and better protect themselves and their children from the risks and dangers associated with App use both on and offline. Having spent almost 3 years studying cyber security in detail and having considered strongly a project where we simply displayed our ability to implement security into an App, our group instead felt that we would like to give back something to cyber security which provides a useful resource to our community both locally and nationally.

3.2 Research Question

Our project offers 3 questions that we will seek to answer via detailed research.

1.
2. Does unfiltered on-line access to on-line content via Apps present a risk to children, or indeed adults?

3. Are there adequate resources available, presented in a convenient user-friendly manner which enable a relatively novice user to implement procedures or settings that would reduce any risks posed by unfiltered on-line access to on-line content via Apps.

4. Is there a demand for said resources?

In answering this question, we will present ourselves a challenge. Do tools exist that will facilitate us in fulfil such a demand. Do we possess the skills to present the resources in a user-friendly manner? We will attempt to meet this challenge in the most professional manner possible

3.3 Project Goals

Our goal is to attempt to answer the questions posed by our research project. We will attempt to do this by analysing relevant data sets obtained by government endorsed resources, recognized professional bodies and charities, research carried out by our group and statistical analysis of App store related data.

In doing so, we aim to present ourselves with a challenge that will allow us to use the skills we have obtained during our journey through the fascinating world of cyber security to fulfil the need, should one exist, for a resource that provides the necessary information required to reduce risks, should they exist, pertaining to unfiltered access online content via Apps.

Should we succeed in justifying both the demand for such resources, and having researched and drawn up recommendations to reduce the aforementioned risks, we shall endeavour to implement said resources and present them via an online platform as our practical product of our theoretical research paper.

3.4 Summary

Our project aimed to investigate App safety, particularly as it pertains to children online. Our primary research question then was, are there risks involved with unfiltered access to online content via Apps? Our group felt that with online data breaches, and scares such as the recent MOMO[2] global phenomenon become more common, the time was right to address what appears to be a lack of understanding of basic precautions and preventative measures which exist in common popular Apps which can help reduce the risks surrounding access to online content. We addressed this question by evaluating quantitatively derived statistics from publicly available research. We began by considering the annual reports released by CyberSafeIreland **(CyberSafeIreland, 2019)**. The statistics in the reports highlight that many children possess their own mobile devices giving them easy access to online content via Apps particularly social media Apps and are exposed to strangers regularly. Furthermore, children are often not speaking to parents about online safety. Teachers too are reporting consistently having to address online incidents caused by access to online content via Apps in the school environment. Having also held information sessions offering tips and advice regarding online security, 53% of parents surveyed felt only 'quite able' to implement these tips. We feel that this research shows that there is a risk concerning unfiltered access to online content via Apps.

In order to show this information was both valid, current and therefore, relevant, we conducted our own research via a survey, as show in sections 8.3 and 8.4 of this document, designed to help narrow our focus to the most popular Apps on the most popular platform. This research confirmed the findings of CyberSafeIreland as being accurate and relevant to our target demo graph. The survey did help to narrow our focus as desired, showing that the mobile platform eclipsed the desktop platform by a large margin. Given the price point difference between Apple devices and Android devices, a preference towards Android devices was expected as their lower price point allows for easier access. However, such a huge difference, with Android showing a big lead in popularity, eclipsing Apple devices by a margin of 50%, was not anticipated. This told us that our focus should be in the mobile platform, and specifically the Android mobile devices. Lastly the survey helped to determine which Apps we should focus on. YouTube showed itself a clear leader in popularity, with Snapchat, Instagram, and WhatsApp also scoring high in popularity statistics. Since security is the primary concern, we also felt we should cover YouTube Kids under the umbrella of YouTube.

An interesting point was raised during the survey, in which we allowed for feedback from participants. Several parents reported their desire to see parental controls added to either Apps or devices. This raised a question among our group. Should we cover security Apps too? While this was initially felt to be out of scope, as it transpired, a security App came up as part of our research and was required to meet the demands of one of our Apps setup processes. This App, Google Family-Link was covered under the umbrella of the App which required it, YouTube. This allowed us to address this parental control concern without straying beyond our scope.

Next, we undertook a case study highlighting some of the areas of risks relating to unfiltered access to online content. We showed through statistics from Talos, Cisco's security group, how much rogue data is sent facilitating the phishing of data from users. These statistics showed that roughly 85% of all traffic monitored by Talos within a month period was spam or inappropriate content aimed at phishing **(Cisco , 2019)**. We further highlighted some specific cases of predator behaviour. One such case we covered showed how a Canadian national befriended through social media, a young Irish girl and travelled to

[2] The global phenomenon MOMO was an internet-based scare alleged to have transpired in social media Apps such as WhatsApp, in which a scary mysterious figure, contacts children to convince them to self-harm. This topic is covered and cited in depth in our case study section.

Ireland on several occasions to have intimate relations with the young victim. This research was felt to justify our project.
With our projects primary research question answered we moved on to some secondary research questions. Do services exist that offer information aimed at addressing the risks of unfiltered access to online content via Apps? If so, is the content enough? Is it easy to access?

To answer these questions, we began our research at the Department of Justice and & Equality's cybercrime website **(Department of Justice & Equality, Cybercrime 2019)**. We discovered that the government offers several services up as well as initiatives and a portal service to host link to access these services. Each of these services was investigated and we found that area of the risks associated with online safety are well documented. Tips and advice are plentiful, if not always easy to find. However, in the specific area of recommendations on how to adjust the settings within Apps, we found a worrying lack of coverage or information. One resource, Webwise.ie did specifically tackle the issue of in App settings but the coverage was minimal at best. Another resource, Hotline.ie refers to content filtering and monitoring Apps which is useful but does not address the issue of what to do once an App is installed. This is the area our service will cover. Our research also highlighted the government's action plan and progress reports which directly covered their acknowledgement that more services are needed, and they intend to add them. This lack of information from pre-existing services lends further justification to our research. We then developed a simple App safety rating guide which is designed to allow us to assign an easy to understand safety score to each App once our recommended settings are in place.

Having shown that the risks exist, and that information relating to how best to adjust the settings in Apps is minimal at best, we began a thorough investigation of our selected Apps. We began with by investigating each Apps terms & conditions. These can be very difficult to read through, but we felt that they contained very important information. We filtered the content down to highlight the specific areas we felt would be of concern to parents to show why they should always read through an Apps terms & conditions to best understand how to deal with any incidents of bullying for example that may occur. Next, we examined the Apps features, to show what the App could do. This we felt would allow a parent to better understand an App and why their child may wish to use it. This facilitates the ability to make informed decisions, weighing up the risks against the potential benefits of an App. We then took users on a step by step guide through the Apps settings. This we feel offers parents a clear breakdown of what can be done in an App, which emphasis on what is safe and what could present a potential risk.

Finally, we offered up our recommended best practice settings and assigned the App a safety score based off having these recommendations in place.

The next step of our project was to produce a WordPress blog with contained and offered up our research material in a user friendly, efficient and easy to access manner. We designed our platform with UI/UX usability in mind. The blog was designed to be simple, presentable, with information easy to find. We undertook a use case test having the usability of our site tested by several volunteer parents who helped highlight areas they felt usability to be lacking.

Our conclusions tied all our research together. They determined there are risks related to unfiltered access to online content via Apps and that while services do exist that cover the area of online safety the specific area of in-App settings is inadequately covered, as documented in our feasibility study in section 6.0 which covers the resources that are recommended by the Irish government and how they are inadequate and our literature review in section 8.0 of our document where we review the statistics and case studies relating to the risks of unfiltered access to online content via Apps mostly pertaining to children.

In documenting this, we show we have answered our research questions while also justifying the demand for the service we propose.

We provided a blog which fills this need by displaying all our research relating to the risks of unfiltered access to online content via Apps simply and effectively. In documenting all our research and going live with the website we complete our goals of delivering a well-researched document which incorporates the results of our survey. The combination of both serve to provide the information which forms the content of our website which we then documented.

We documented our analytic results of traffic on the website using Google Analytics to monitor traffic, page hits, and new versus returning users.

3.5 Methodology

Our methods will be based on the quantitative analysis of multiple data sets. These data sets will be extracted from statistical studies which adopt a scientific approach to the collection of data from demo graphs that relate to our target demo graph, which is both parents in Ireland, and children in Ireland.

We will begin by analysing relevant data from a study or studies which cover the area of child safety online and the risks associate with App use. We will select the papers and studies we shall analyse from those resources recommended by the Irish Government, and leading recognized charities specializing in this area of online cyber security and child safety.

This initial data set will be used to develop a study of our own, which shall be distributed to our target audience locally and if possible, nationally via social media, although this will need to be done very carefully in order not to pollute our data set with replies from outside our target demo graph. This study shall be comprised of a survey which shall determine if the information collected corelates, thereby verifying the relevance of our first data set. The statistics will be crucial in determining the age groups of children at risk. As well as the platforms we focus on, the App types we study.

Finally, we shall gather a third data set via statistical analysis of the App stores of both Android devices, and Apple devices to determine if we see any correlating statistical quantitative patterns. The analytical and confirmative approach will allow us to ensure that the data points we extract from our data sets are relevant, current and applicable to our target audience.

This will allow us to determine which Apps we shall study. Having selected our Apps, we shall begin a case study into the risks associated with unfiltered access to online content via Apps. While the scope of the study will be global and wide ranging, we shall attempt where possible to focus our attention nationally and on incidents pertaining to the Apps we have elected to study. This will again be a quantitative study. We shall highlight several known areas of vulnerability and focus into some specific cases which further serve to highlight the risks of unfiltered access to online content via Apps. These case studies will serve to help justify the need for our service. Having served to confirm the risks exist we will then move on to reducing risks.

Our blog which we shall propose, will be based around offering up guides which we believe will reduce the user profile visibility, and thus the user's online footprint. This will make it harder for the user to be approached, contacted or solicited by unwanted users. This will also reduce the risk of abuse such as bullying or even contact by online predators or otherwise malicious users. These guides will be based on analysing the terms and conditions to highlight how each parent companies views and deals with serious abuse or breaches of their terms and conditions. We will further highlight areas pertaining to data sharing as the general data protection regulation **(GDPR 2019)** has now come into effect.

The features and most importantly the App setup (where applicable) and settings will be covered in detail. We shall offer up the settings we believe to be the most secure which will provide the reduced visibility and online footprint which shall serve to provide a greater level of safety for children and indeed parents online. This information will be presented via our WordPress blog in a simple, easy to access no frills manner.

3.6 Research Goals

3.6.1 Initial Justification Based Research

We will determine whether a risk exists surrounding children's or adults unfiltered access to online material via Apps and if a risk exists, develop recommendations on how to reduce the extent of such risks.

We will first research the use of social media, games, messaging or Apps that encompass a wide audience such as streaming services. The types of Apps that we will research will be determined based on the statistical evidence. We will search for pre-existing research which falls into this category as well as any existing marketing statistical data which will aid in our decision-making process.

Using this research, we will design a survey specifically aimed at parents and children which will determine firstly if survey participants agree that there are security concerns surrounding Apps and if they feel they should be concerned about children's online security and visibility.

Should it serve to vastly increase the security of the Apps being covered, we may briefly discuss VPN's and explain how this might increase the security of users online.

We will seek feedback regarding the usability of security options or features. Are they easy to find? Are they easy to understand? We shall seek to determine if children are more likely to be using their own personal accounts or where personal accounts are not being used, would they have access to parental accounts on their parent or supervisor's devices.

Next, we will determine the platform or platforms we should narrow our focus too. Furthermore, we will use this survey to determine if age is relevant to child App use and if so, use this data point as a guiding principle when developing our recommendations regarding the severity of the security practices. Lastly, we will provide a comments section to see if there are any areas pertaining to online security that participants, be they adult or child are interested in having us cover that we may have over looked. From this research we shall select several Apps to investigate.

3.6.2 Case Study: Unfiltered Apps – What are the risks?

A case study will be performed to determine the level of risk regarding general App use. Close attention will be shown to the Apps we select to scrutinize in detail. We shall delve into some of the more widely known scandals. We will be looking to investigate inappropriate content becoming available to users who may not wish to view this content, or have their children view it.
Another area of obvious concern is online predators. We will be closely examining the potential for this kind of activity and how one may reduce it with the proper implementation of our recommendations if possible. Alongside predators another form of malicious use of Apps, particularly where social media Apps are concerned is online abuse, verbally, via comment sections or direct messaging.

3.6.3 App Safety System

Combing the data gathered from our initial research as well as our case study, with the knowledge and experience we have gained during our studies of cyber security we shall develop an App safety rating system which shall determine the level of safety, or risk if any, of each of the Apps we research. Our App will be a 10-point system. The system shall be visually represented, and each App will be assigned its score via a colour coded chart that allows users to easily identify the level of risk associated with the App in question.

3.6.4 App research

Using the Apps we selected from our initial research, we will investigate what features each App has and its functionality. We will investigate each Apps terms & conditions along with their privacy policies to see how personal data is stored and used by the App.

We will then review the security features and settings each App has and recommend the safety configuration of settings which we feel will reduce online visibility and the user's footprint making it harder for marketing agencies or product manufacturers to gain access to user's data, while also reducing the likely hood that online malicious users or predators will be able to find and contact the user. We will conclude this portion of the project by evaluating each App according to our App safety rating system and offering our recommendation as to whether that App should be used by children or not.

3.6.5 Blog

Design and implement a useable web-based WordPress blog which shall be live by project conclusion. The Blog will be based purely on the research conducted in our project and will lay out the recommendations proposed in an easy to read manner that is accessible to all levels of computer user from novice to advanced users.

4.0: Scope and Reasoning

4.1 Initial Research

Our research shall be limited first by location. We shall restrict our research to information pertinent to the Irish Consumer base. Any third-party research material or statistics must be based on research or statistics from the Irish marketplace only where possible. Our survey will therefore be presented only to Irish consumers. International based research and statistics in relation to App use may result in our recommendations being less relevant to our target audience, which is the Irish market and more specifically, parents in Ireland.

Secondly, our research will be limited by App type. We will initially focus on social media, games, messaging or Apps that encompass a wide audience such as streaming services that prove popular based on statistical research. However, should any App be discovered during our research that serves to drastically impact positively upon the security of an App currently being covered or indeed all App use, our scope will be extended to cover this App as part of the leading Apps research.

4.2 Case Study

One exception shall be made in relation to our case study or case studies. While culture differences may push one App to the top of one marketplace, where as another may top the user charts in another location, based on a different demographic, the same risks will apply to App use in general. As such, our risk assessment case study or studies will be global in scope with a narrow focus on the impact within the Irish borders where possible.

We will limit our research in our case studies to non-tool (software tool) based malicious interactions or social engineering. Any abuse, or access gained using the manipulation of a program's coding, database or online systems shall be deemed out of scope, as such 'hacks' would be their very nature, bypass any appropriate security settings.

Any content which may be deemed inappropriate and is gained or enhanced through improper application of provided security settings shall be of immediate concern. Inappropriate market targeting shall also be considered in scope.

We believe that unfiltered access to online material via Apps constitutes a very real and present risk to children and will seek to prove this in our case study or studies by providing documented evidence of such dangers or concerns related to such dangers.

4.3 Researching App Terms & Conditions

We shall start our research by examining each App's terms & conditions. Each App's privacy policy shall be considered part of the terms & conditions as will data-sharing. Within the terms & conditions for each App our specific focus will be to highlight areas that we feel may be of concern to users or parents of users where it pertains to account security or user related data. Any areas of the terms & conditions that do not directly impact the security, integrity or sharing of user data shall be considered out of scope. This research will be performed as we feel most users do not perform an in-depth analysis of terms & conditions **(Byrne S. 2019).** Therefore, we shall seek to condense material we find relevant to security or privacy and present this information in a condensed form. This may facilitate us reproducing content verbatim from the Apps website, though we shall try to limit this were possible.

4.4 Researching App Features & Settings

We shall cover all features of each App that specifically pertains to security or may have some form of impact on the account security, integrity or user visibility. Some potential risks pertaining to data sharing may overlap between terms & conditions and features. We will be sure to cover these topics in at least one of these areas.

Where features are discovered which do not help the user to better understand the product enabling better security practices to be applied, and these features do not carry with them direct security implications, we will not cover these features if we feel it is too far out of scope.

We will cover all security settings provided by each App which may help secure the account pertaining but not limited to integrity, sharing of user data and user visibility. We will then design recommendations to achieve the optimum security settings to better protect the user while using the App.

Should any App require the use of a secondary App, such as for example a VPN
or a third-party program, this secondary or third-party App will be covered and considered part of the leadings Apps research, in so far as it must be covered to achieve the desired level of protection. While our intention will be to avoid tangent branches of research, we cannot avoid potential avenues of research that may provide a greater level of overall security, whether inside settings or externally of the Apps we cover.

Regarding the number of Apps to be covered, we feel that in order to deliver quality content we must limit our Apps to be researched to a manageable level initially (though should the project be extended beyond college, this could be expanded). Therefore, we shall limit ourselves to a minimum of three Apps and a maximum of five. This allows us an achievable goal with room to expand should we deem it in scope.

Apps will be rated according to our safety rating system based on our research. No external considerations shall be covered in the reasoning of our rating. Finally, we will reflect upon each of our Apps and give based on the inherit risk or lack thereof, recommend whether the App should be used be children.

Research goal justification

We believe that our initial research will provide a solid foundation which will guide us in narrowing the focus of all research to follow. In narrowing the focus to the Irish consumer market, we ensure that not only is information upon which our blog is based relevant to its target audience, but also falls in line with, while also expanding upon resources offered by other services. Furthermore, by limiting the Apps to those our research tells us are popular among our target audience we further ensure the relevance of the content.

Our case study will serve to highlight the risks relating to unfiltered access to online content via Apps. This is crucial as it is of course the primary reasoning behind why our group feels our service is needed. While it shall not be the only justification for our project it is the primary justification for our service. If no risk exists, then no service is needed.

In researching, in depth, the terms & conditions of each App to a greater degree than other services have done we shall serve to highlight the import of content contained therein, while also demonstrating that ignorance of the terms & conditions can lead to further risks. For example, not knowing what data is being collected may lead to not knowing what data you must try to prevent being collected if such data presents a risk. This will necessitate some copying of the terms & condition verbatim from the Apps covered although we shall where ever possible aim to distil the content down such that it is easier to present in a condensed form. This will also necessitate a disclaimer within our blog, detailing that our condensed form of terms & conditions is not recognized by the App providers and are not binding. We will also state that our intention is not to discourage readers from investigating terms & conditions but highlight the importance of investigating them.

App features

In researching App features, we will cover what an App can do, and how to reduce the impact of the features where they may present a potential risk. This is the heart of our service. We will provide breakdowns of the Apps so that parents may make informed decisions about whether they or their child should be using an App. Should they decide to use an App, they will be far more informed of the risks thanks to our case study and our settings guides shall provide detailed walkthroughs on what our group believes constitutes the safest way to reduce the risks associated with unfiltered access to online content via Apps, while also reducing a user's online visibility and footprint. All of this will allow us to create a user friendly, informative service which offers up easy to understand guides in a manner that is easy to access and meets the goal of increasing the security and online safety of children and parents.

4.5 Blog

Our blog content will be solely based on the research and recommendations we will perform. It will be designed using WordPress and usability and presentability will be a key factor in the design process. WordPress plugin modules will be considered within scope for the design process but not essential. Usability being a key factor we will strive to make sure the website is not overly complicated but demonstrates our ability to incorporate UI/UX.

While the blog may contain hyperlinks, we don't intend to implement much interactivity if any. Our goal here is to present information as the users may user or not as the case may be. The blog is a resource not a tool.

We felt like we needed to make a blog because it allows us to transform our research and results into something that is easy to understand in order learn how to implement the recommendations we will make. Dissemination of the information can only be achieved if the information is simple to understand and easy to access.

5.0 Deliverables

Herein is listed our project deliverables:

1. Survey: The survey covering our desired research material it will primarily be used to gather data required to produce the report. Where required, we will report the findings of the data to justify our decisions, but we will not include data points deemed irrelevant to the selection process (To be documented in our report).

2. Detailed research report: Our report will include all documentation pertaining to the research material and the design and implementation of our blog. This documentation will include a case study on the dangers of social media specifically pertaining to cases or reports involving children. We will choose three to five Apps to research based on popularity and our case study. Our research for each App will be the basic functionality of the App followed by a walkthrough of how to set up the App in the safest manner.

3. WordPress based Blog: Our blog will be hosted online and will be accessible to the public. Should time allow for it, we may seek to attempt to promote it in the hopes of increasing App safety amongst children in Ireland. We will display our walkthroughs for securing each of the covered App on the blog. As well as the risk associated with unfiltered access to online content via Apps and any other information derived from the research carried out during our research phase deemed pertinent to security. Security will be incorporated into our site as well as search engine optimization and Google Analytical data to allow for future work to be carried out based of relevant data sets that do not require us to collect user's personal data to remain GDPR compliant.

6.0 Feasibility Study

Our search began with a visit to the Department of Justice & Equality, Cybercrime website **(Cybercrime 2018)**, to document the listed resources and government endorsed websites offering further resources. And we find that the Irish government has made significant strides towards tackling the area of cybercrime and indeed the area of child endangerment online which is commendable.

Directive 2011/93/EU

Article 25 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography deals with 'Measures against websites containing or disseminating child pornography'. The activities of Hotline.ie and the Garda blocking initiative together fulfil Article 25 in Ireland. Cybercrime oversees these activities. The remainder of the Directive has been transposed into Irish law.

Hotline.ie provides a secure, confidential service for the public to report suspected illegal content on the internet.

The aim of the Garda Blocking Initiative is to block access to child sexual abuse material (CSAM) on the internet in Ireland. An Garda Síochána (AGS) signed a Memorandum of Understanding with a company, under which the company agreed to block access to CSAM. AGS is actively engaging with further providers in order to extend this initiative.

Figure 1 Hotline initiate as documented on The Department of Justice & Equalities website, ***(Department of Justice & Equality 2019) [Accessed March 2019]***

As seen above, the first resource offered is perhaps one of the most important resources., Hotline.ie **(Hotline.ie 2019).** Hotline serves as both a protection resource, but more importantly it serves as a first point of contact for victims who may wish to report crimes anonymously or for those who suspect they may have discovered illegal content that needs to be reported.

Next, The Department of Justice & Equality lays out its action plan for tackling the area of online safety going forward from 2018-19. This action plan is wide ranging and sweeping in scope, however, its very existence highlights the ongoing efforts of our government to tackle this problem and continue to offer and promote services such as the platform we propose to offer.

Action Plan for Online Safety 2018-2019

Online safety is being tackled in a coordinated manner by the Government's first Action Plan for Online Safety, which was launched by the Taoiseach in July 2018. The Action Plan reflects a whole of Government approach and contains twenty-five actions under five main goals. The actions are assigned to six different Government Departments for implementation, including this Department.

This Department's main actions under the Plan include:

- We will legislate for new criminal offences with the support of the Oireachtas.
- We will strengthen links and processes with industry for removing illegal and harmful material.
- We will work with online platforms based in Ireland to advance online safety measures.
- We will work with EU and international partners to actively promote online safety.

Each actions is further broken down into constituent elements and the full plan can be viewed here: Action Plan for Online Safety 2018-2019

The Action Plan is overseen by a Sponsors Group consisting of representatives of the six Departments involved in the Plan and by the National Advisory Council on Online Safety (NACOS). NACOS comprises key stakeholders and is chaired by the Minister of State at the Department of Communications, Climate Action and Environment.

A report by the Sponsors Group on progress made on the Action Plan during 2018 is available here: Action Plan for Online Safety 2018 Progress Report

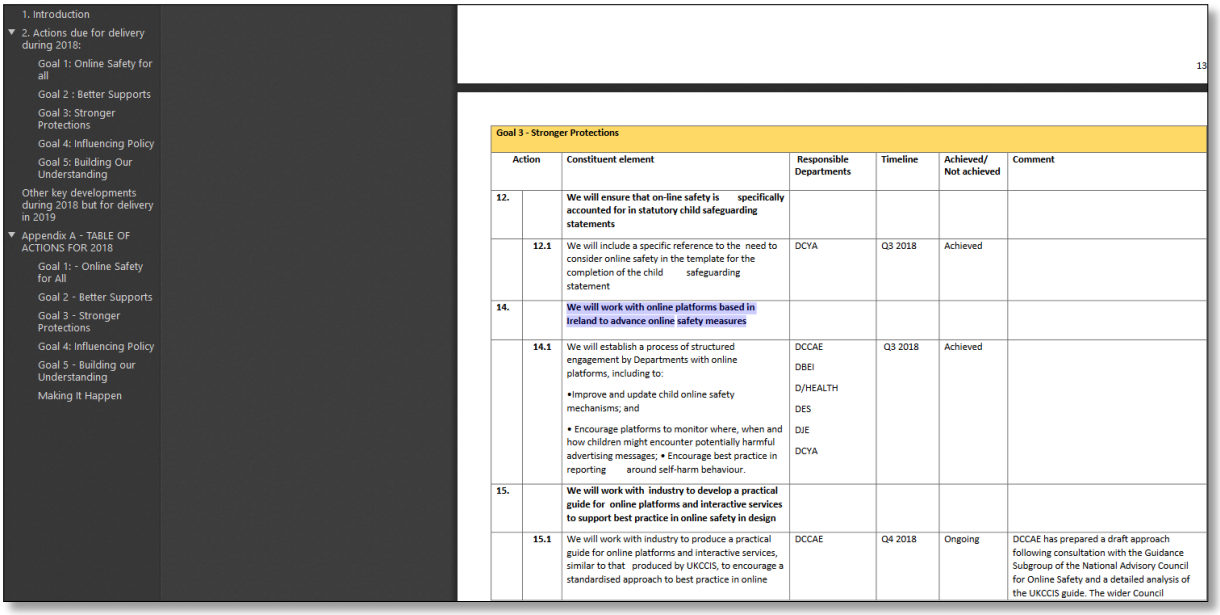
A report by the NACOS on progress made on the Action Plan during 2018 is available here: National Advisory Council for Online Safety Progress Report 2019

A single online access point has been established as part of the gov.ie portal which provides pathways to information on online safety.

Figure 2 Action plan establish by The Department of Justice & Equalities website, ***(Ibid) [Accessed March 2019]***

This action plan determines to legislate for new criminal offense that will support the efforts of the Oireachtas to tackle these crimes, strengthen links with industry experts and content providers to further the removing of harmful and illegal content, and increase online safety measures and finally, work with EU & international partners to actively promote online safety. The action plan in its entirety can be accessed below **(Department of Justice & Equality – Online Action Plan 2018).**

While our platform does not offer this facility in a live environment our research and recommendations are based precisely off this type of research, on some of the most popular Apps at the time of researching. This could be adapted at a later stage to include live updates based on up to date Apps and social networking platforms should there be a demand for us to expand our services beyond this college project.



1. Introduction
2. Actions due for delivery during 2018:
   - Goal 1: Online Safety for all
   - Goal 2 : Better Supports
   - Goal 3: Stronger Protections
   - Goal 4: Influencing Policy
   - Goal 5: Building Our Understanding
Other key developments during 2018 but for delivery in 2019
Appendix A - TABLE OF ACTIONS FOR 2018
   - Goal 1: - Online Safety for All
   - Goal 2 - Better Supports
   - Goal 3 - Stronger Protections
   - Goal 4: Influencing Policy
   - Goal 5 - Building our Understanding
   - Making It Happen

13

Goal 3 - Stronger Protections

Action		Constituent element	Responsible Departments	Timeline	Achieved/ Not achieved	Comment
12.		**We will ensure that on-line safety is specifically accounted for in statutory child safeguarding statements**				
	12.1	We will include a specific reference to the need to consider online safety in the template for the completion of the child safeguarding statement	DCYA	Q3 2018	Achieved	
14.		**We will work with online platforms based in Ireland to advance online safety measures**				
	14.1	We will establish a process of structured engagement by Departments with online platforms, including to: •Improve and update child online safety mechanisms; and • Encourage platforms to monitor where, when and how children might encounter potentially harmful advertising messages; • Encourage best practice in reporting around self-harm behaviour.	DCCAE DBEI D/HEALTH DES DJE DCYA	Q3 2018	Achieved	
15.		**We will work with industry to develop a practical guide for online platforms and interactive services to support best practice in online safety in design**				
	15.1	We will work with industry to produce a practical guide for online platforms and interactive services, similar to that produced by UKCCIS, to encourage a standardised approach to best practice in online	DCCAE	Q4 2018	Ongoing	DCCAE has prepared a draft approach following consultation with the Guidance Subgroup of the National Advisory Council for Online Safety and a detailed analysis of the UKCCIS guide. The wider Council

Figure 3 Progress report published by The Department of Justice & Equality ***(Department of Justice & Equality – Progress Report on Action Plan for Online Safety 2018) [Accessed March 2019]****.*

A progress report is also offered which can be accessed here **(Department of Justice & Equality – Progress Report on Action Plan for Online Safety 2018)**. Contained within that progress report's Appendix A, Goal 3, section 14.1 is the following statement: 'We work with Online platforms in Ireland to advance online safety measures. The section further states that improved mechanisms and platforms that monitor where, when and how children encounter harmful messaging and content are needed. This shows the governments awareness that more resources are needed. This lends justification to the need for our service.

Next up, the cybercrime department offer a single access point to the Gov.ie portal. This portal is the access point to the government's safety awareness campaign BeSafeOnline **(BeSafeOnline 2019)**. This portal contains a large volume of information via links to resources for both parents, children and the general population relating to addressing and tackling inappropriate content such as:

- Online bullying internet safety booklet
- Sexting
- Online Pornography
- Online Gaming
- Grooming/Sexual Exploitation
- Tips for parents
- Helplines
- Mental health awareness
- Top Tips

Figure 4 The gov.ie portal link to the BeSafeOnline awareness campaign as documented on The Department of Justice & Equalities website, ***(Department of Justice & Equality 2019) [Accessed March 2019]***

The next listed resource offered by The Department of Justice & Equality cybercrime division falls under the umbrella of the EU safer internet Ireland initiative. This initiative aims to combat illegal, harmful and predatory use of the internet. The project partners with several online resources such as:

- Webwise.ie: a developmental platform service aimed primarily at providing resources for Teachers
- Hotline.ie (which we have already mentioned): This service is operated by the Internet Services Providers Association of Ireland (ISPAI)
- ISPCC Childline: The Irish Society for the Prevention of Cruelty to Children (ISPCC) which operates the well-known helpline for children and has expanded its support network into helping with online issues.
- NPC Primary: The National Parents Council Primary operates the parent/adult helpline, including cyber bullying, offering online and offline training course

EU Safer Internet Ireland

Combatting illegal, harmful and predatory use of the internet requires responses at national, EU and international levels. Ireland is part of the EU Safer Internet initiative. As part of the initiative, Ireland provides awareness raising, helplines and a hotline. These services are provided by partner organisations, with Cybercrime providing coordination.

The project partners are:

- **Webwise.ie** This is part of the PDST (Professional Development Service for Teachers) Technology in Education in the Department of Education and Skills. It deals with awareness raising, develops materials and programmes for schools and runs the annual event for Safer Internet Day in Ireland.
- **Hotline.ie** The Internet Service Providers' Association of Ireland (ISPAI) operates the hotline, the service which allows the public to report suspected illegal content or activities found on the internet.
- **ISPCC Childline** The Irish Society for the Prevention of Cruelty to Children (ISPCC) operates the helpline (Childine), which provides services on a 24/7 basis where children affected by issues encountered on the internet may turn for advice and guidance.
- **NPC Primary** The National Parents Council Primary operates the parent/adult helpline, a dedicated helpline to deal with issues relating to internet safety, including cyberbullying. The NPC also provides parents with training courses, both online and face to face.

The project partners are co-financed by the European Union's Connecting Europe Facility.

Figure 5 The EU Safer Ireland Initiative resources as documented on The Department of Justice & Equalities website, ***(Department of Justice & Equality 2019) [Accessed March 2019]***

Finally, the cybercrime division highlights, draws attention to the Internet Safety Day. This event is put together by the joint Insafe-INHOPE network with the support of the European Commission. With funding from the Connecting Europe Facility Programme and takes place annually in February. The individual events that take place over the course of The Internet Safety Day are organized by Webwise.ie, and information pertaining to the event is found on the Webwise.ie website.

Safer Internet Day

This international event takes place every February to promote safe and responsible use of the internet and mobile phone technologies, especially amongst children and young people.

Safer Internet Day is organised by the joint Insafe-INHOPE network with the support of the European Commission, with funding provided by the Connecting Europe Facility Programme.

The annual Irish national Safer Internet Day events are organised by Webwise.ie. For information on events and activities in Ireland to mark Safer Internet Day, please see www.saferinternetday.ie

For details of European and worldwide events, please see www.saferinternetday.org

Figure 6 Internet Safety Day, as documented on The Department of Justice & Equalities website, ***(Department of Justice & Equality 2019) [Accessed March 2019]***

One further resource which is note-worthy, is CyberSafeIreland, Irelands leading online safety charity. While not endorsed by the Irish Government, we believe that CyberSafeIreland's contributions to this field of online preventative child protection services are huge and we shall reference and cover their work in detail during our literature review.

Having reviewed the recommendations of the Irish Government & CyberSafeIreland we examined these resources and information offered by each, focusing on information and services which relate to the field of online security and safety.

6.1 Hotline.ie

Where online security and risk reduction offers some fantastic resources, as seen below.

Figure 7 Information & services n offered by Hotline.ie related to Online secirity and risk reduction. ***(Hotline.ie – Internet Safety 2019)[Accessed March 2019]***

One of the most important services Hotline.ie offers is the ability to report content anonymously. Very few agencies other than An Garda Siochana offer this facility making it an absolutely invaluable resource.

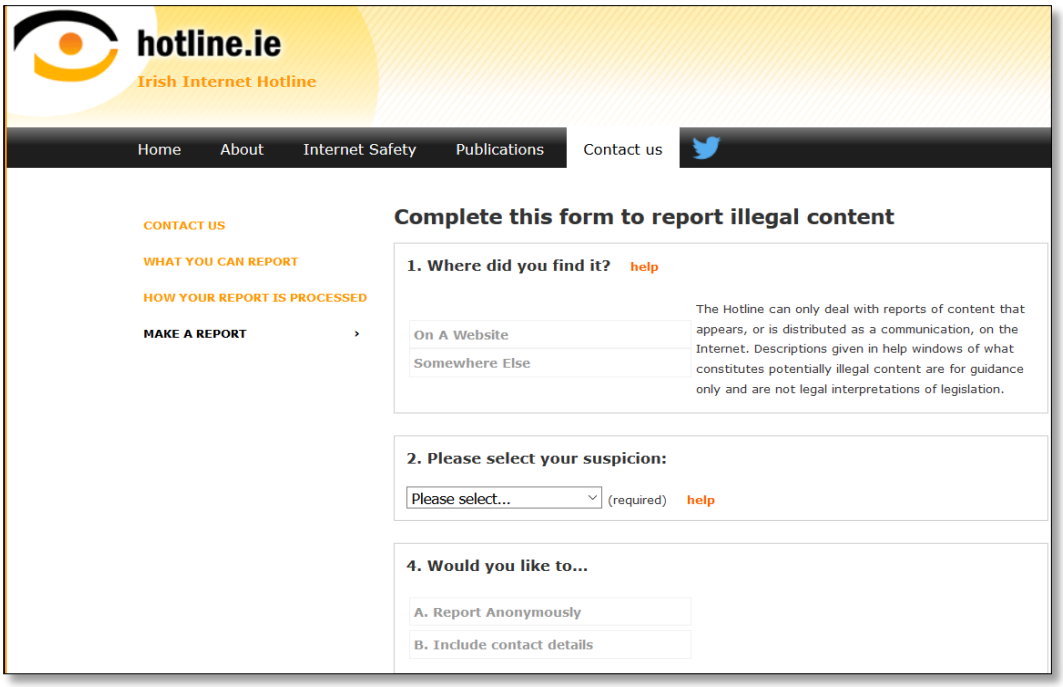


Figure 8 Hotline.ie report content feature. ***(Hotline.ie – Make a Report 2019)[Accessed March 2019]***

Hotline.ie goes on to offer tips. These tips while certainly useful, centre around parenting tips external to actual device being used. Furthermore, they offer links to some of their Internet Safety Awareness partners such as Webwise.ie and Childline. The basic guidelines centre around location of devices, communication skills, mindfulness and supervision combined with setting rules for children, relating to their App or device use. They do not even mention in App or device settings.

Basics...

- Keep the computer where you can see it in a busy part of the house - not in the child's bedroom!
- Don't forget about laptops and smart phones!
- Spend time online and familiarise yourself with websites and games they use.
- Look and take note if too much time is being spent online.

Talk about...

- Protecting privacy, don't allow your child to give out personal information such as phone numbers, addresses, passwords, etc.
- Behaving appropriately when using social networks and online chat, etc.
- Being careful who they accept as friends online. For younger children it should be other kids they already know from school or the neighbourhood.
- "Think before you click!" when uploading photos or videos. That is, asking yourself "would I like this photo/video to be online if it was me in the picture?

Be Watchful...

- Find out what your children's habits are regarding social media platforms.
- Strangers online can be hard to spot. Familiarise yourself with whom your child is talking online. Who are their "friends"?
- Check history files for suitability of visited sites and chat rooms (especially for younger children).
- Check e-mails (especially for younger children).
- Check mobile phone usage. Talk to your mobile provider about dual access or other parental controls they offer - even for prepaid (credit) customers.

Set Rules...

- When the internet can be accessed and for how long.
- Never give out personal information without permission.
- Never agree to meet an online friend without permission.

Figure 9 General online safety tips offered by Hotline.ie ***(Hotline.ie – Safety Tips 2019)[Accessed March 2019]***

While the general safety tips covered by Hotline.ie are fantastic tips that should be followed by parents about parental supervision external to a child's device or account, it's also true that no parent can supervise a child's activity 24 hours a day. Help is needed to cover those times when a parent cannot be physically present to monitor and manage activity.

Regarding specific general breakdowns of popular Apps, as well recommendations about the specific risks of these popular Apps, Hotline.ie offers almost no information. This is perhaps understandable, relying instead on its partners to cover this content. However, Hotline.ie does recommend some third-party security Apps that do afford some ability to incorporate filtering of Apps and content into your device, or child's device; whilst not giving any specific details or information on how to setup and maintain the use of said Apps.

Figure 10 Hotline.ie filtering services advice and recommendations page ***(Hotline.ie – Filtering Software 2019)[Accessed March 2019].***

The Filter Apps recommended are as follows:

- UPC Magic Desktop [Online]: http://www.upc.ie
- KidSafe [Online]: http://www.kidSafe.ie
- Net Nanny [Online]: http://www.netnanny.ie
- Cyberpatro [Online]l: http://www.cyberpatrol.com
- Eset Smart Security: http://www.eset.ie
- PearlEcho: http://www.pearlsw.com
- Safetica Endpoint Security [Online]**:** http://www.safetica.ie
- Websense [Online]**:** http://www.websense.com
- SafeScreen [Online]**:** http://www.pixalert.com

Each of these Apps offers a range of security features which vary from App to App, from localized content blocking and filtering to remote content blocking and filtering, location tracking and data-monitoring as well in relation to online activity. Some even include advanced features to identify likely pornographic material. However, having visited each Apps website and examining the feature sets we found that many of these websites are down and the ones still active are a bit too technical for parents or children with little technical device or cyber security experience and instructions where not exactly user friendly.

We felt a much more verbose, well documented setup and installation guides, not to mention settings recommendations would have provided a much better user-friendly experience.

These content filtering Apps serve a vital role in child protection online, however, they do not cover in App settings where Apps or content have been allowed. Almost none allow live monitoring of activity and none prepare a parent or child for the risks associated with other user's intent for data that an unprotected account may leak, such as photos or video. Our group acknowledges and commends Hotline.ie's role in the fight for greater child protection online, but we feel there exists a gap in their coverage we can potentially fill.

6.2 BeSafeOnline

The Gov.ie portal 'BeSafeOnline' **[BeSafeOnline, 2019]** acts as a container for links to the Internet Safety Awareness initiatives partner resources. As such it offers no self-contained resources. While our group feels that it would be of great benefit to parents to have our platform included in this repository of links, we do not feel that the portal has any impact, be it positive or negative to the feasibility of our project.

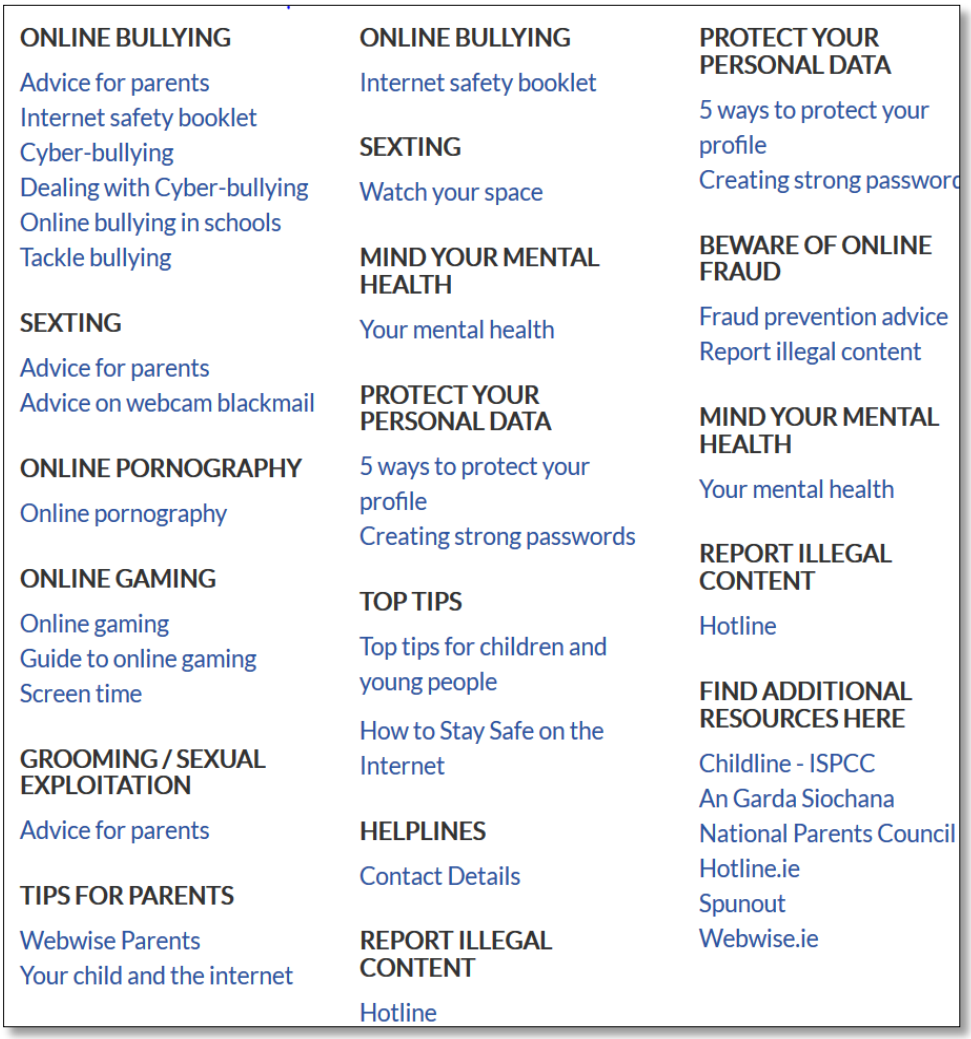


Figure 11 Sample of links offered by the Gov.ie portal service BeSafeOnline ***(Gov.ie 2019) [Accessed March].***

6.3 Webwise.ie

Webwise.ie offers resources regarding online safety, in the form of videos, articles, tips and featurettes primarily aimed at teachers, also parents to a limited degree. This is due to the limited size of the team at Webwise.ie which is acknowledged on their website.

Figure 12 Webwise.ie homepage ***(Webwise.ie 2019) [Accessed March 2019].***

Seen above, on the top left we have the Parent, Teacher and Youth menus. While in the centre of the page we have essentially the same menus, however the content contained therein is slightly expanded. The difference we find is the top left menu offers resources by category, where the centre menus do not. We found the top left menus more useable and navigable.

The top right of the screen, seen below, offers resources such as BeInCtrl, which is a government backed initiative aimed at tackling the risks associated with online activity. Lockers, which aims to provide schools with resources to tackle issues such as online bullying, and UP2US which is a further anti bullying initiative.

Figure 13 Webwise.ie homepage, get Resources link ***(Webwise.ie 2019) [Accessed March 2019].***

Next up the Webwise offers a section covering tips and trending content. The user interface experience in this section was simple, well laid out and easy to navigate with current trending stories and tips offered up immediately and a link to more presented under top stories.

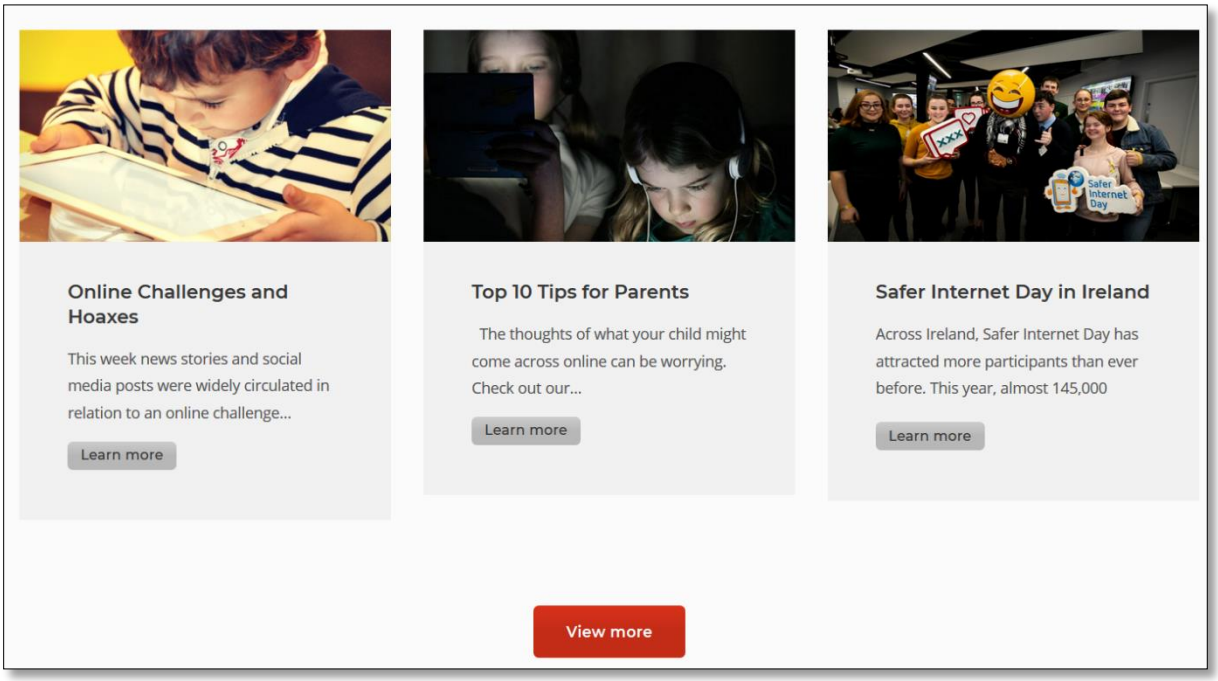


Figure 14 Tips and trending content offered by Webwise.ie ***(Webwise.ie 2019) [Accessed March 2019].***

Next, we see the first section of any website or resource we have seen which begins to touch upon the areas we feel are lacking in resources and information available, which is to say, App breakdowns, guides, and analysis.

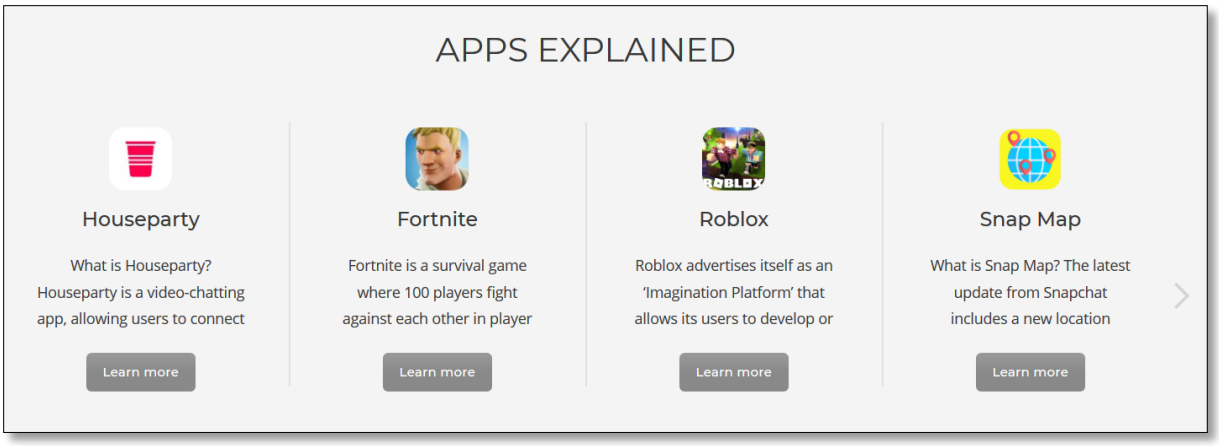


Figure 15 Webwise.ie homepage, Apps explained section ***(Webwise.ie 2019) [Accessed March 2019].***

This section covers Apps, App updates games social media platforms and other App's believed to be of relevance to teachers and parents.

Webwise goes on to offer up a resource and information and training section for teachers.

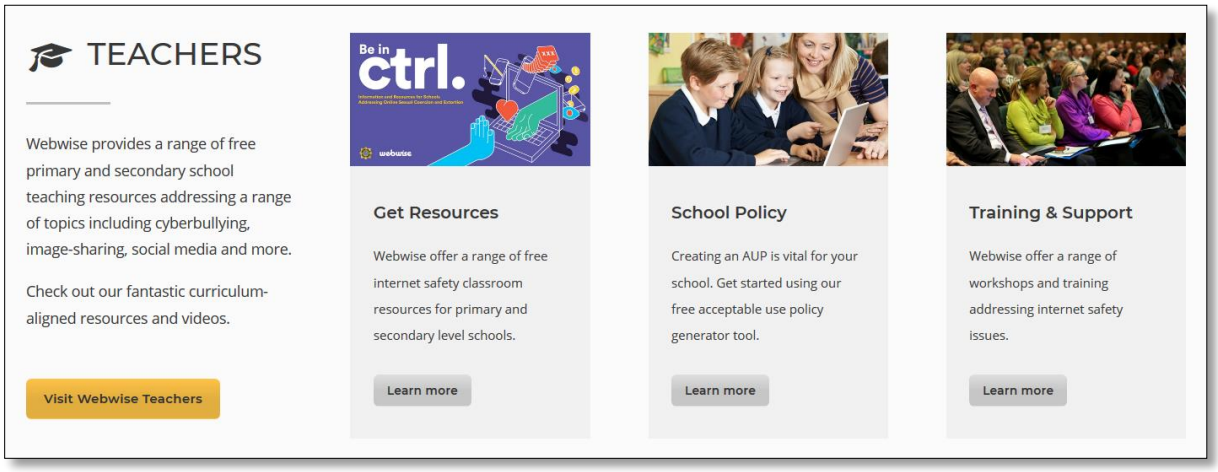


Figure 16 Webwise.ie homepage teachers resource information and training links ***(Ibid) [Accessed March 2019].***

Followed immediately by similar links aimed offering parents the opportunity to get resources, consult chat directly with webwise staff or get advice.

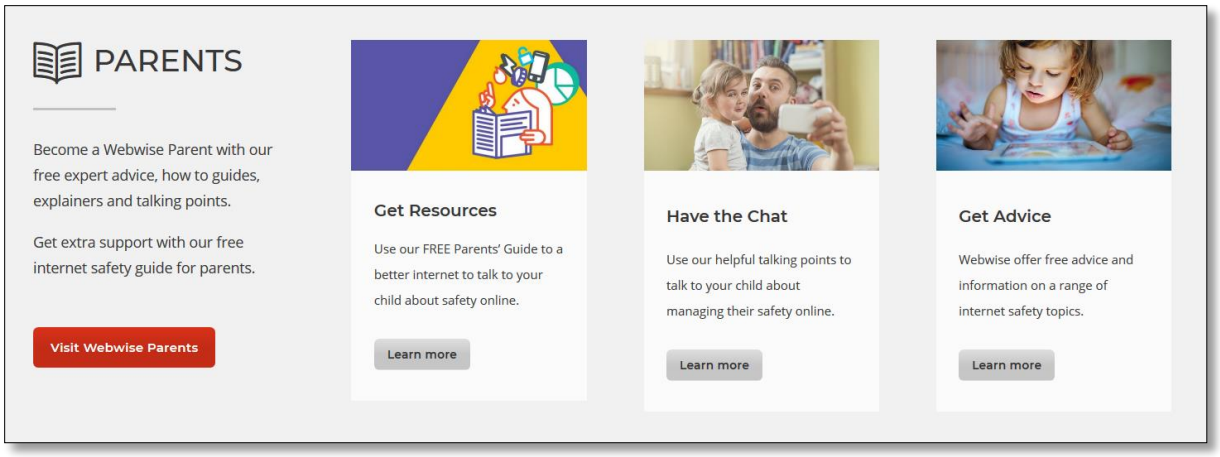


Figure 17 Webwise.ie homepage parents resource chat and advice links ***(Ibid) [Accessed March 2019].***

While the interface layout did change slightly here, which we felt it served to further add a sense of confusion to the overall layout of the website, usability remained high with content easy to navigate from the home page.

Lastly, Webwise.ie offers a direct media link highlighting its video resources. What is fantastic about these resources is that it is immediately apparent that people who are organising the webwise content have heavily included children in the content creation process. This is something often overlooked. Once again, usability remains high.

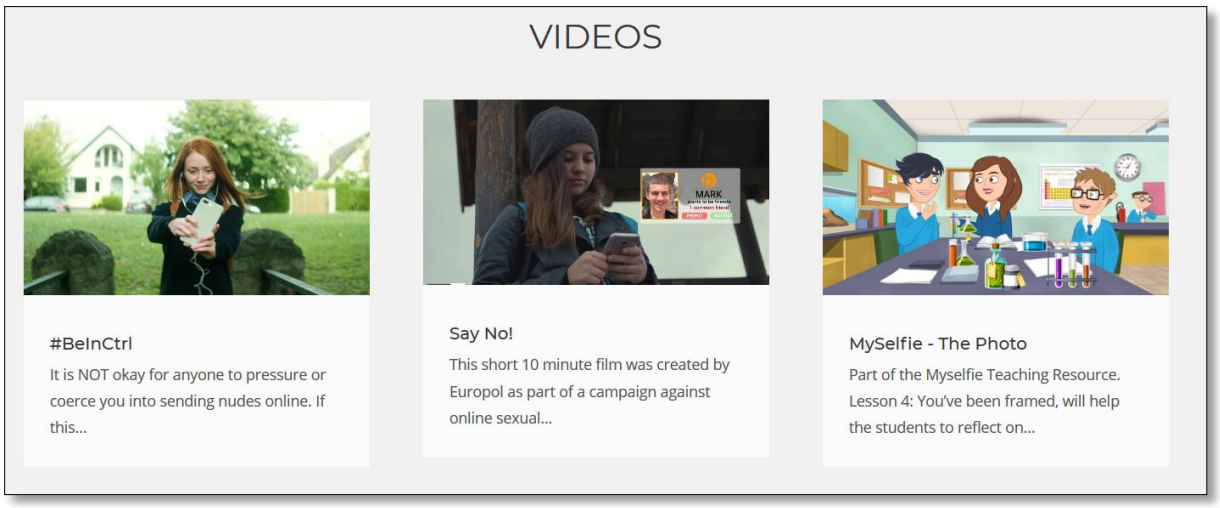


Figure 18 14 Webwise.ie homepage Teachers video media links ***(Ibid) [Accessed March 2019].***

Overall, usability is high, however our group did feel that the layout created a slight air of confusion to how the content was presented. It was further concluded that the homepage contained some unnecessary overlap with some content repetition in multiple menus this is the primary source of confusion in content layout.

Having delved into each section in detail, while we commend Webwise.ie on its deep range of advice regarding the classroom environment, and its tips regarding parental approaches and attitudes towards governing a child's use of Apps and devices, We find the primary focus of Webwise.ie is in dealing with issues external to a device or App, or interpersonal social skills within a particular platform type such as social media.

Very little information is offered up with regard to setting guideline and recommendations. That being said, Webwise.ie does offer a specific 'Apps Explained' section so we shall examine this section further as it enters into the area the blog we propose to produce will cover.

And here, in 'Apps Explained' is where Webwise.ie really begins to offer practical breakdowns of Apps, which we feel help to allow parents to make informed decisions regarding whether their child should or should not be using an App which Webwise.ie have covered. Their breakdowns cover features, in some cases risks and some information is offered regarding adjusting settings to reduce inherent risks where the risks are covered. However, it must be stressed we feel that this information is lacking any real in-depth coverage.

The Apps currently covered by Webwise cover some of the more popular Apps used in the Ireland, for example, Snapchat, WhatsApp, YouTube and Minecraft. Some of the more obscure Apps such as 'ooVoo', which is particularly commendable and highlights that particular effort has been made to ensure that as few parents as possible are left struggling to be able to relate to and understand their child's online activity. In an effort to determine if Webwise.ie's coverage of Apps undermined our proposal we elected examine the breakdown of two popular Apps.

6.4 WhatsApp as featured by Webwise.ie

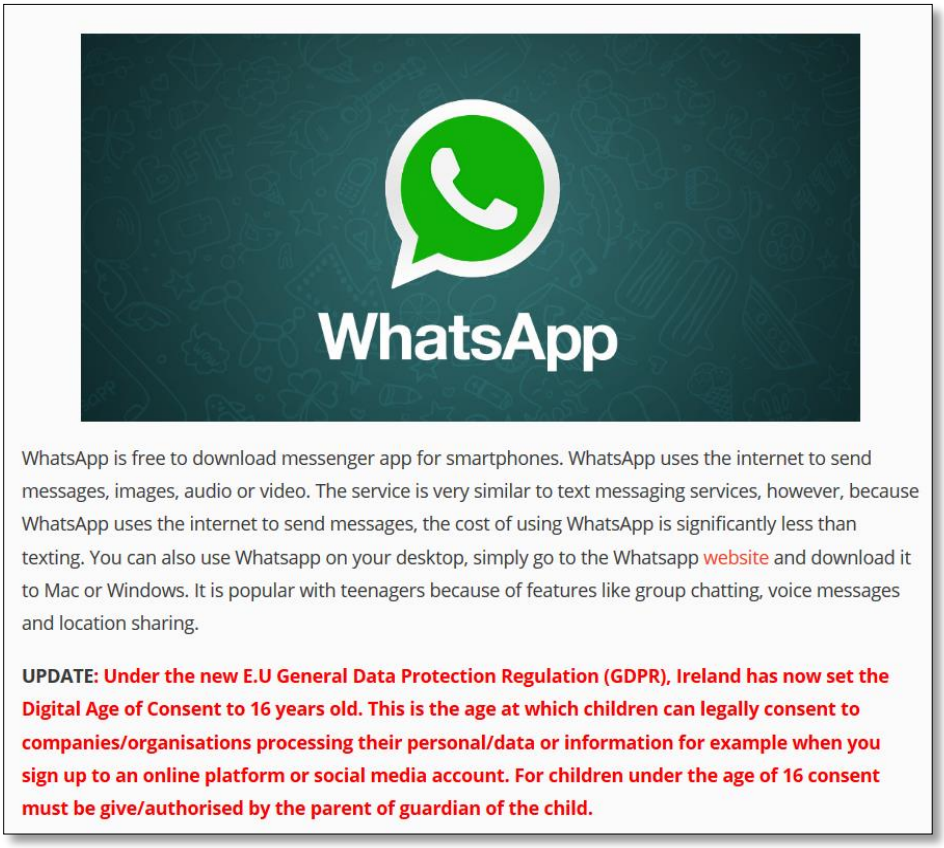


Figure 19 Breakdown of WhatsApp App by Webwise.ie ***(Webwise.ie 2019) [Accessed March 2019].***

Here, we see the initial breakdown of WhatsApp. As we see the age of digital consent has been updated given the recent bill raised in the Oireachtas proposed the digital age of consent should be 13 and was amended to 16. This shows that Webwise.ie's content is being keep up to date which is of course vital if the information being offered is to remain relevant. While the features of WhatsApp are briefly mentioned, we find that the breath of features is not fully covered. While the risks associated with WhatsApp are barely mentioned at all. Attention is drawn to the possibility of charges relating to data roaming but none is drawn to dangers of online grooming, data sharing or phishing. We find this to a shocking oversight.

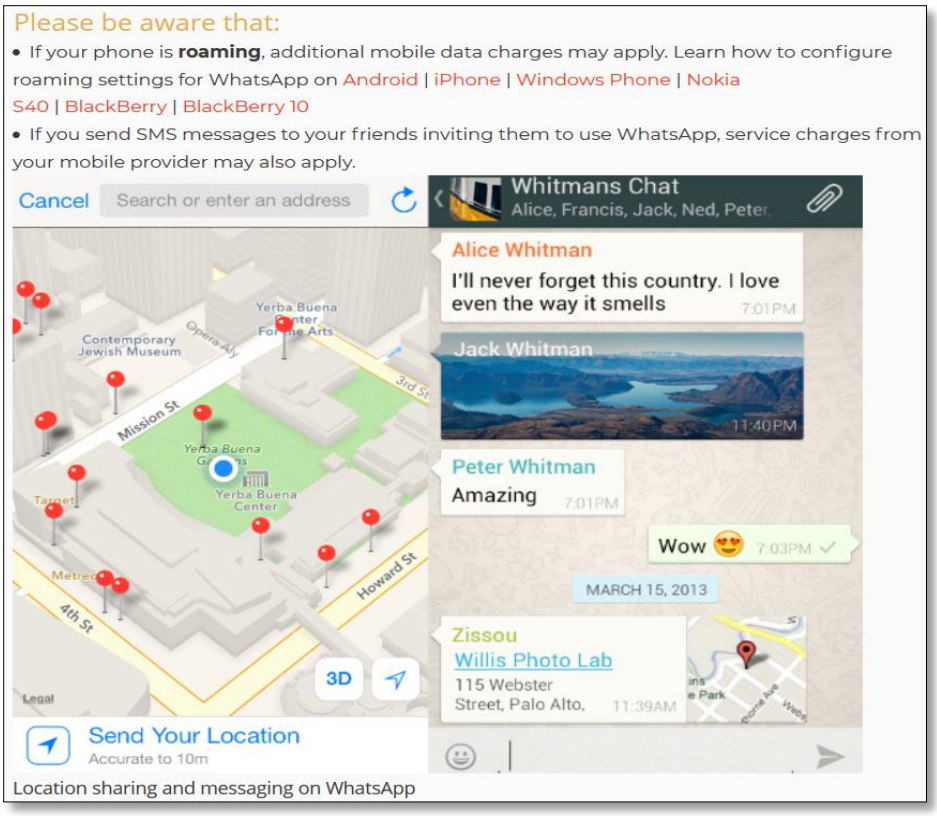
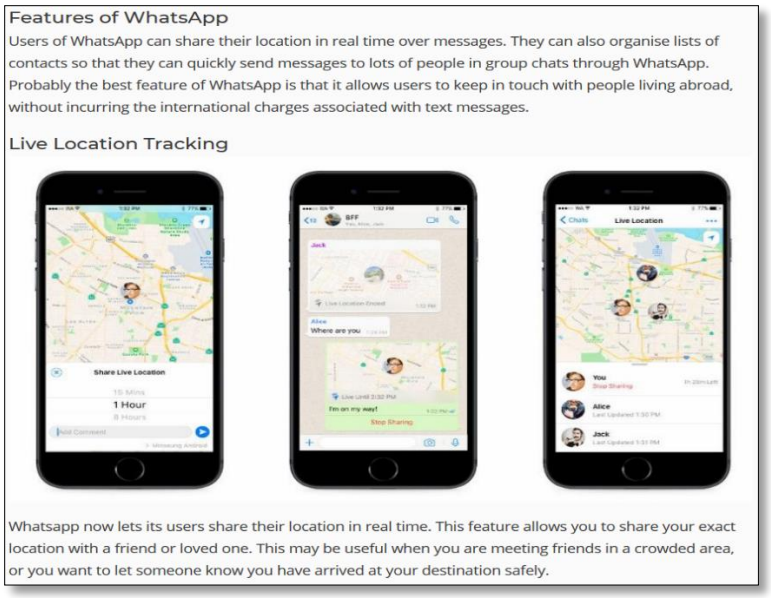


Figure 20 Webwise featuring WhatsApp features warning of possible costs relating to data roaming ***(Ibid) [Accessed March 2019].***

Webwise.ie does try to draw attention to features relating to GPS tracking data, but not the dangers of such technology, as it pertains particularly to children.



Features of WhatsApp

Users of WhatsApp can share their location in real time over messages. They can also organise lists of contacts so that they can quickly send messages to lots of people in group chats through WhatsApp. Probably the best feature of WhatsApp is that it allows users to keep in touch with people living abroad, without incurring the international charges associated with text messages.

Live Location Tracking

Whatsapp now lets its users share their location in real time. This feature allows you to share your exact location with a friend or loved one. This may be useful when you are meeting friends in a crowded area, or you want to let someone know you have arrived at your destination safely.

Figure 21 Webwise Draws attention to the GPRS tracking feature contained within WhatsApp ***(Ibid) [Accessed March 2019].***

Webwise.ie goes on to document how to enable location sharing, but again does not cover the risks. While also documenting the content editing feature which allows users to remove content locally and remotely from all device attached to a group chat.

What is strange is that Webwise elected to cover the settings on an IOS device. While provided no data as to why. This appears odd to our group, as publicly available statistics, as well as our own data sets reveal that android is far more popular than Apple devices as our data sets will reveal in our research section.

To use it you:

1. Open the contact you would like to share your location with
2. For IoS select the + button, and for android select the paperclip on the lower left-hand side of your screen
3. Choose 'Location'
4. When the map appears, select the 'Share Live Location' option
5. You will then see this message '*Participants in this chat will see your location in real-time. This feature shares your location for the duration even if you're not using the app. You can stop sharing at any time'.*
6. You can then decide how long you would like to share your real-time location with this person, you have the option of 15 Minutes, 1 Hour or 8 Hours.

It is important to know that you are **allowing your movements to be tracked by another person**. Only use this feature with people you know and trust. Parents should talk to their child about location sharing and advise them against it.

Editing Features

WhatsApp have also added the ability to delete messages that you may have sent in error. This may be helpful if you sent a message to the wrong contact. The next update to the messaging service will look at adding a 'Reply Privately' function while in a group chat.

WhatsApp users can also now hold down a message in a group chat to select and add a reply to it. It ensures that members in a group can follow conversations more easily and respond to specific questions in a group chat or write comments on content in the group.

Figure 22 Webwise docments enabling locations sharing on an IOS device, and editing feature ***(Ibid) [Accessed March 2019].***

Finally, Webwise.ie makes a brief reference to WhatsApp terms & conditions. With a note on how to change your age-based restrictions which will alter slightly your account visibility within the App settings. This is the entire extent of the settings-based recommendation and indeed the coverage of the impact of the settings offered by the App regarding security.

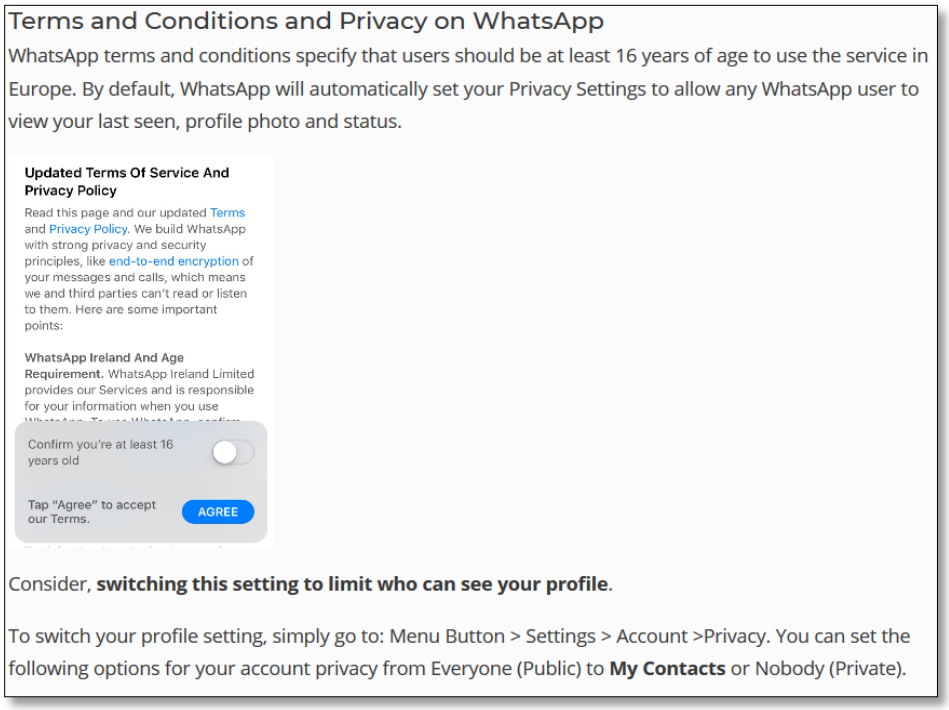
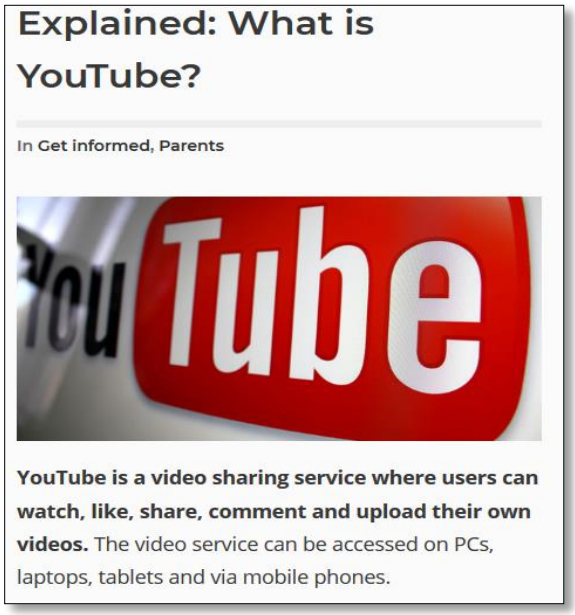


Figure 23 Webwise.ie coverage of age-based account visibility related settings in WhatsApp ***(Ibid) [Accessed March 2019].***

6.5 YouTube as featured by Webwise.ie

Webwise begins once again be giving a brief breakdown of what The YouTube App is. This explanation is brief, yet to the point.



Explained: What is YouTube?

In Get informed, Parents

YouTube is a video sharing service where users can watch, like, share, comment and upload their own videos. The video service can be accessed on PCs, laptops, tablets and via mobile phones.

Figure 24 Webwise.ie explains what YouTube is, Apps explained section ***(Webwise.ie 2019) [Accessed March 2019].***

Next, Webwise.ie breaks down the feature of YouTube, and here we felt that perhaps the feature breakdown is perhaps a little lacking.

What Are the Main Functions of YouTube?

- Users can search for and watch videos
- Create a personal YouTube channel
- Upload videos to your channel
- Like/Comment/share other YouTube videos
- Users can subscribe/follow other YouTube channels and users
- Create playlists to organize videos and group videos together

Figure 25 Webwise.ie covers the features of YouTube in a very minimalist fashion ***(Ibid) [Accessed March 2019].***

Age restriction are addressed, where by Webwise.ie draws attention to the fact that users under 16 should not be accessing the YouTube service under the terms & conditions set by YouTube.

Age Restrictions

To set up a YouTube account users must be 18 years of age or 13+ with parental consent. **Update: Under the new E.U General Data Protection Regulation (GDPR), Ireland has now set the Digital Age of Consent to 16 years old. This means young people under the age of 16 in Ireland are not allowed to access this platform.**

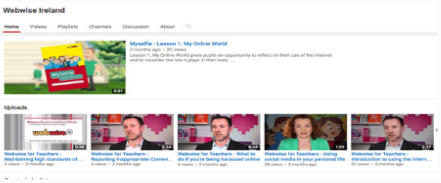
However, users do not need to sign-in to access the website or to view videos. There is, however, a YouTube kids version now available to download for free. YouTube kids is designed for children aged 3-8 years old and make it easier for children and parents to find content they are interested in. Click here for more info the YouTube Kids app.

Figure 26 Webwise.ie covers YouTubes age restriction ***(Ibid) [Accessed March 2019].***

Next, Webwise.ie covers the risks associated with YouTube use, focusing in on the areas of inappropriate content, and cyber bullying.

What Are the Risks?

YouTube is a great place to discover new things, learn and get entertainment, however, there are some things parents and teens should be aware of when using the service.



Inappropriate Content

YouTube has over a billion users and with an estimated 300 hours of footage uploaded per minute, not all of it is appropriate for children.

But you can help minimise the risk of your child encountering content that may not be appropriate for them. If you or your child sees something inappropriate, users can flag the video with YouTube. For more info on flagging inappropriate content go to: google.com/youtube/

Figure 27 Webwise.ie covers the risks associated with inappropriate content being displayed within YouTube ***(Ibid) [Accessed March 2019].***

Cyber Bullying

Unfortunately, people can experience negative comments and bullying on the service particularly through the comments function (YouTube users can comment on other users videos). If your child has a YouTube channel/profile it might be a good idea to recommend they disable comments on their own profile/channel. This can be done very easily via settings and helps minimise risk of experiencing negative comments. If your child is experiencing harassment on YouTube, you can block and report users.

See below for more info on reporting and blocking users

Block Users: google.com/youtube/block

Report Abuse: youtube.com/reportabuse

Figure 28 Webwise.ie covers the risks of cyberbullying associated with YouTube use ***(Ibid) [Accessed March 2019].***

Finally, Webwise.ie covers some resources offered by Google which cover how to set up parental controls as well as managing privacy settings. As well as YouTube's in-built safety mode and how to disable comments.

Tips for Keeping your Child Safe on YouTube

1. Managing Privacy Settings

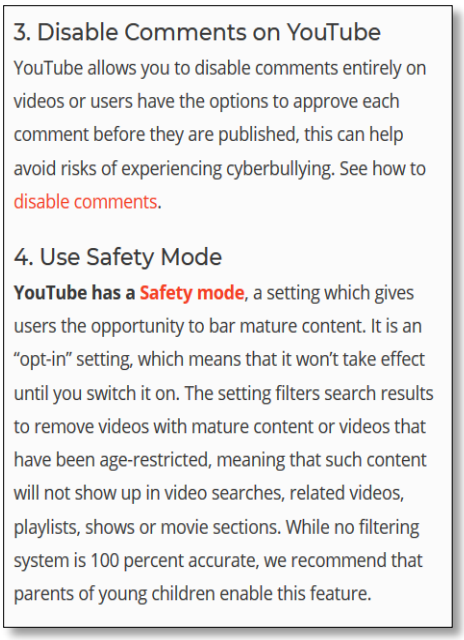
When a user uploads a video to YouTube, by default the video is set to public, which means anyone can see the video. Depending on the age of your child, you should discuss what settings are best to use if your child is uploading footage to YouTube. You can easily switch videos to private or unlisted (published on YouTube but cannot be found without a direct link to the video).

You can also invite people to view your videos using Google Circles. Please note, you need to link your channel with Google+ in order to share a private video with other users. Click here for info on how to connect a YouTube channel to a Google+ profile.

2. Set up Parental Controls

Parents should set up age restrictions and parental controls on YouTube. See how to set up parental controls.

Figure 29 Webwise.ie covers privacy settings and parental controls ***(Ibid) [Accessed March 2019].***



3. Disable Comments on YouTube

YouTube allows you to disable comments entirely on videos or users have the options to approve each comment before they are published, this can help avoid risks of experiencing cyberbullying. See how to disable comments.

4. Use Safety Mode

YouTube has a Safety mode, a setting which gives users the opportunity to bar mature content. It is an "opt-in" setting, which means that it won't take effect until you switch it on. The setting filters search results to remove videos with mature content or videos that have been age-restricted, meaning that such content will not show up in video searches, related videos, playlists, shows or movie sections. While no filtering system is 100 percent accurate, we recommend that parents of young children enable this feature.

Figure 30 Webwise.ie draws attention to the ability to disable comments and YouTube's Safety Mode ***(Ibid) [Accessed March 2019].***

While our group recognizes that the primary area of focus addressed by Webwise.ie is education and offers information training for educators and tips for parents, we find that the coverage of Apps and particularly features, risks and recommendations regarding security and the reduction of user's account visibility and online footprint lacking.

We feel that this is the specific area on which we can improve upon. Our platform will be focused on providing parents with information relating to a full breakdown of some of the most popular Apps, the features contained therein and coverage of the settings and recommendations as to how to best reduce the user's exposure to any potential risks.

6.6 ISPCC – Childline

The ISPCC operates the emergency child welfare service Childline, which serves a critical role in helping both children and parents address and attempt to prevent harm both physical and mental to children. However, Childline takes a broad approach to the subject. While it does offer some tips and advice centred around online activity, its coverage of this area is minimal and as such we do not feel it has any positive or negative impact upon the feasibility of our project.

6.7 NPC Primary

The NPC primary is a resource like Webwise.ie which is specifically focused in face to face training. As part of its training program it does offer training courses centred around online safety. However, its online resources are extremely limited. In fact, its entire resource catalogue amounts to a video archive of guides pertaining to online safety.

It seems clear that while this information is pertinent to parents, providing parents with information can be described as a secondary role at best. And the NPC Primary's delivery of training, resources and information is conducted primarily during face to face training.

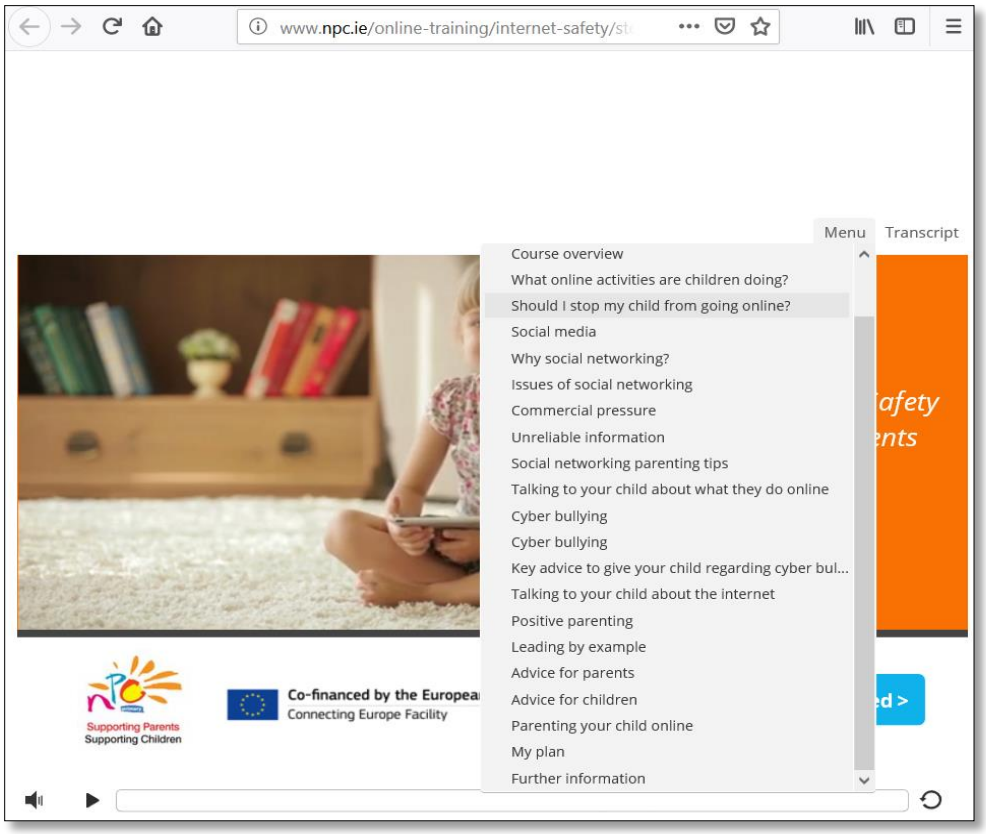


Figure 31 The NPC Primary's online video catalogue of guides related to internet safety ***(WWW.npc.IE) [Accessed March 2019].***

6.8 CyberSafeIreland

CyberSafeIreland is Irelands leading internet safety non-profit charity, supported and funded by leading contributors to the area of cyber security such as Trend Micro, Permanent TSB and COMMSec. As a charity it does not fall under the umbrella of being part of the governments Safety Internet Awareness campaign. We feel this independence is important as it allows for the collection of and comparison of data sets outside of the main government sponsored partners data sets.

The principal action undertaken by CyberSafeIreland is the collection of data, from which it produces a yearly annual report pertaining to children's online activity and the risks associated with it. Its reports are extremely thorough, well researched and recognized by both leading institutions and companies.

While its annual reports are a truly wonderful source of data, gathered from schools ongoing yearly surveys which is presented in a truly user-friendly professional manner. We found its online resources somewhat lacking. Their website does offer tips and resources, but they are primarily in the form of links to the actual support pages of Apps. As is the case seen below.

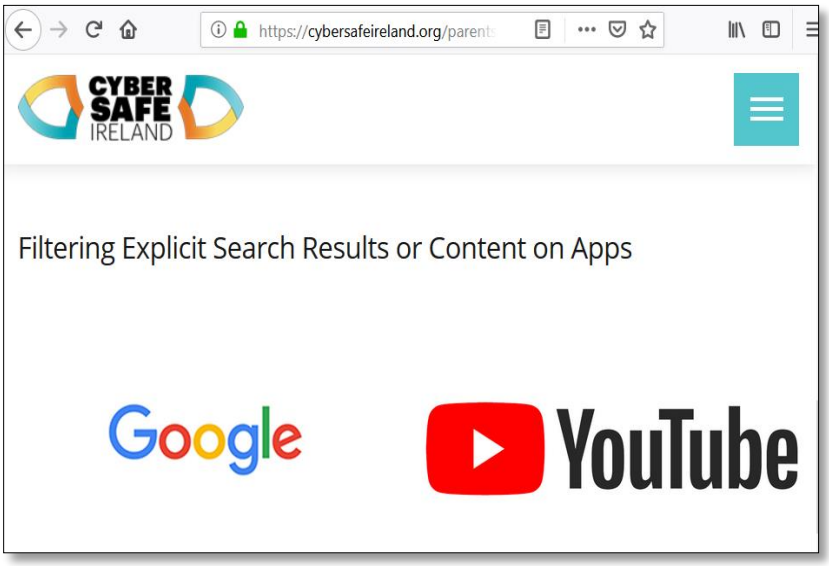


Figure 32 CyberSafeIreland presents links to settings to filter explicit content via Google and YouTube ***(Parental Controls) [Accessed March 2019].***

As we shall see. This links merely link to the Apps support website and do not in fact offer guidance and help.

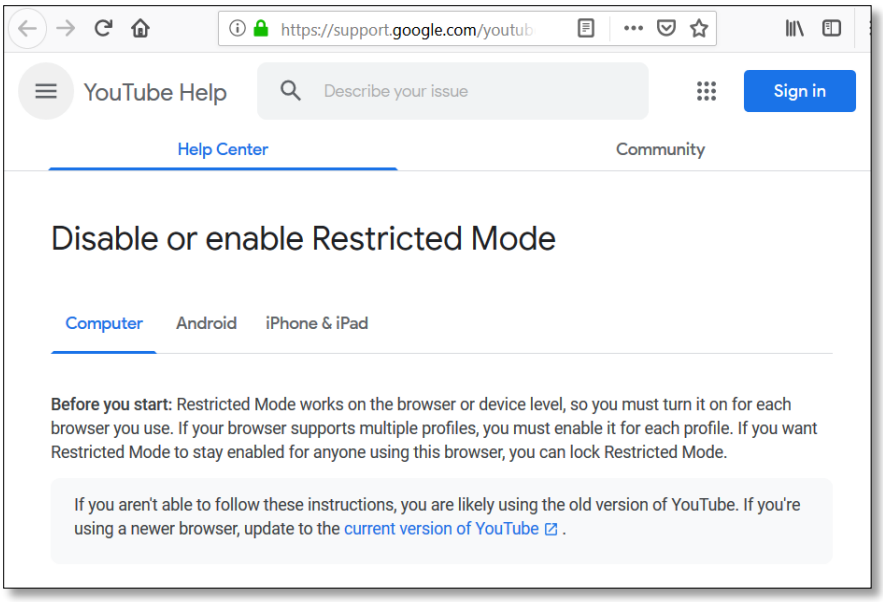


Figure 33 CyberSafeIreland's *link takes us directly to YouTubes Support site* ***(YouTube Help Centre) [Accessed March 2019].***

We find that the CyberSafeIreland does not impact negatively upon the feasibility of our proposed platform. However, we recognize the impact that CyberSafeIreland has in the area of online safety, particularly where children are risk. We found their work to be invaluable.

6.9 Feasibility Study Determination

Our research during our investigation into the feasibility of our proposed platform suggests that while many resources offers tips and recommendations external to devices and Apps, only one officially recognized source attempts to tackle the challenge of breaking Apps down such so that parents can understand them. Furthermore, where the risks associated with each individual App are concerned we also find a severe lack of information or analysis. Lastly, where settings and recommendations to reduce risk, where a risk may exist are concerned, we find that almost no effort is made to cover this subject. These are three areas of lacking services our platform aims to address. Such a service would serve to compliment already existing services and resources and fill a gap in the security coverage related to unfiltered access to content via Apps.

7.0: Proposal

Our group propose to design, develop and implement a blog-based platform online, that will discuss and assess the features, and risks associated with unfiltered or unsupervised access to the features of some of the most popular Apps in Ireland as determined by well documented research, particularly where children are concerned.

We shall break down the features such that parents may better understand their child's desire to use the Apps. And provide a user-friendly understanding into how the features work.

Lastly, our platform will examine the settings of each App we cover and offer what we feel are the most secure settings that will help to reduce the user's visibility, online foot print and exposure to risk, where a risk is identified. Any other pertinent information derived from our research that we feel shall serve to further increase security in this area will be included. The site will include an SSL certification for increase security and the service will be live by project completion. Search engine optimization will be added to facilitate reaching as large an audience as possible and Google analytics shall be included to facilitate future work. Collection of personal information will remain GDPR compliant.

8.0 Literature Review – Unfiltered Access to Apps – What are the risks?

8.1 CyberSafeIreland's 2017/18 Annual Reports

We began our research by looking for the leading groups covering cyber security with emphasis on studying the dangers associated with online App use. Research by such groups covering App use, and the dangers associated with it in relation to children would be of note.

This led us to CyberSafeIreland **(CyberSafeIreland 2018)**. CyberSafeIreland is a recognized charity in Ireland which investigates online safety and produces an annual report covering the previous year with a statistical analysis of Irelands online use. This proved a great starting point in our research.

In 2017, CyberSafeIreland produced its second annual report, stating that 69% of teachers do not feel equipped to teach online safety in the classroom. 32% of children have not discussed online safety with their parents. 16% of children surveyed in 2016 reported they spent more than 4 hours online per day and 216 incidents of bullying were reported in that year. This report was available at the time of writing this report due to an issue with CyberSafeIreland's website however the figures mentioned above were taken directly from the website and not the report. This is not an inconsiderate figure and one can only image how many incidents went unreported, this being only the second year of the survey.

As discussed by Orla Ryan, reporter for the 'The Journal' online **(Ryan O. 2018)**, This report went into far more depth. The report highlighted that 68% of children aged between 8 and 13 own their own smart phone. However, this study being two years old was felt to be a little out of date in the fast-paced evolving world of cyber security. So, we moved on to cover the report released in 2018(**CyberSafeIreland, 2018**), covering 2017.

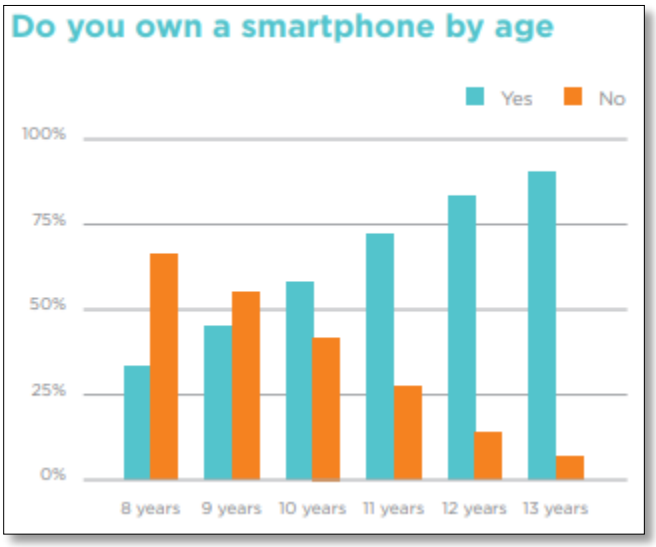


Table 2 Ownership of smartphones by age. 2018 CyberSafeIreland annual report ***(CyberSafeIreland 2018, page 17)****.*

This does not include tablets, so it is reasonable to assume if one where to count tablets this number is higher in terms of the number of children with access to mobile devices. The report also shows that 70% of this age range of children also use social media. This tells us that if a risk is posed by the unfiltered use of App's with online functionality, significantly over half of this age range of children alone are at risk.

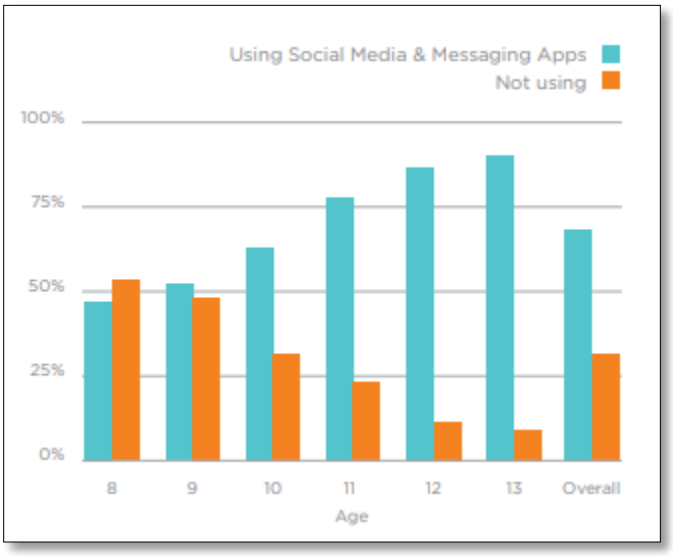


Table 3 Use of Social Media & Messaging Apps among children aged 8 -13. 2018 CyberSafeIreland annual report ***(Ibid) (page 18 2018).***

The report concludes that 32% of children talk to strangers online per week with 18% conversing with strangers each day. Of this group of children who reported contact with strangers, 6% report daily contact, 8% reported contact more than once a week, and a further 4% reported contact less than once per week. While 78% reported no contact with strangers. There is a 2% discrepancy in the figure here which might be explained as a misprint, however we sought to contact CyberSafeIreland regarding this discrepancy but received no response. However, overall, the numbers show that almost 25% of those children survey present a risk of exposure to inappropriate or malicious users while online.

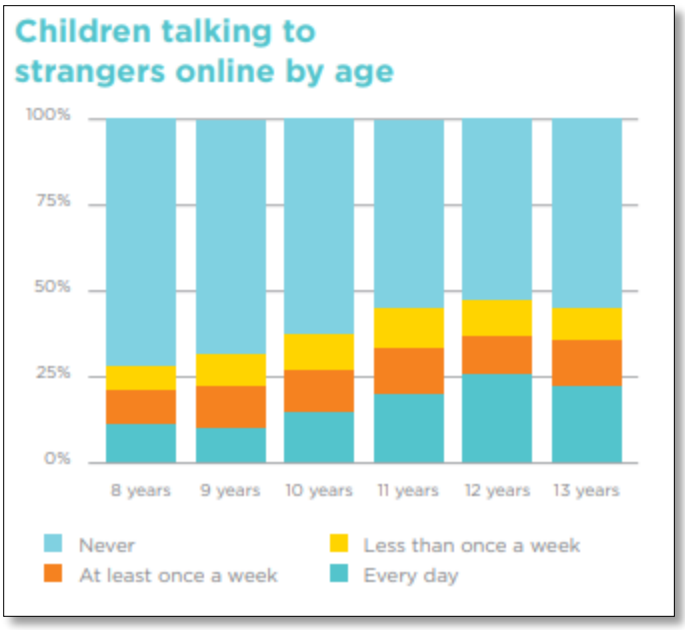


Table 4 Chart of children talking to strangers online listed by age. 2018 CyberSafeIreland annual report ***(Ibid) (page 20 2018).***

This report also found that 30% of children are still not speaking to their parents regarding online safety. This remains consistent and poses a bigger question. Is this consistency due to lack of resources, or ease of access to resources online, or due to currently available resources being difficult to access or understand?

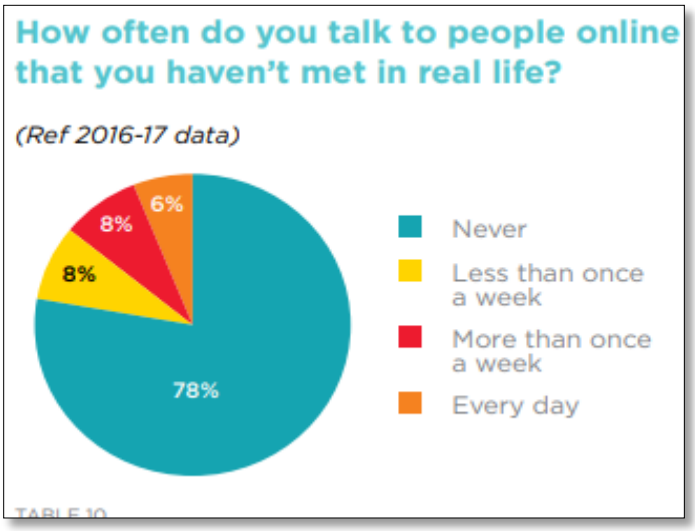


Table 5 Chart of frequency of online contact with strangers among children surveyed. 2018 CyberSafeIreland annual report ***(Ibid) (page 21 2018).***

Also included in the reports data set was a fascinating glimpse into the online incidents that teachers faced and had to deal with. While this data point is very specific and localized to a school environment, it does provide some insight into what parents must also face regarding issues surrounding bullying, harassment, and worse still, inappropriate adult contact with children.

When asked how many incidents teachers had to deal with on a yearly basis, 38% reported none, while 22% reported having to deal with at least 1 incident, 35% had to deal with between 2 and 5 incidents, and 5% had to deal with more than 5 incidents. These numbers show that online safety in schools is an issue educators are facing regularly.

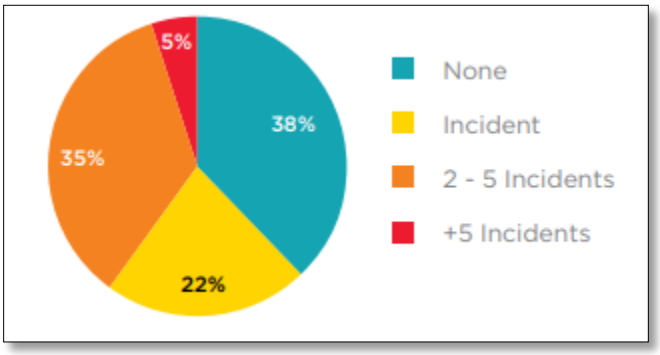


Table 6 Frequency of yearly on-line related incidents faced by teachers regarding their pupils. 2018 CyberSafeIreland annual report ***(Ibid) (page 25 2018).***

Finally, one more highly pertinent data point was found in the annual report. Following the release of the report, CyberSafeIreland undertook a set of information sessions in selected school, to attempt to better inform parents of the risks they felt were very real and present. Having presented these information sessions to parents, CyberSafeIreland then posed a simple question to parents. How confident are you that you can apply the recommendations offered during the information sessions at home?.

53.1% of parents felt quite confident that they could apply these recommendations, 40.6% felt very confident they could apply them and 6.3% felt a little confident they could apply the recommendations offered. This is a quite high success rate, showing the CyberSafeIreland put a lot of thought into the presentation of the information sessions.

When asked if their children tended to speak to them regarding online safety the numbers indicate that children too are sensing a need for awareness of online safety. While a majority reported having spoken to a parent recently the figure could be further broken as follows, 30% reported speaking to a parent within the last year, 24% within the last month and 30% had rarely spoken to parent suggesting they had at some point. But outside of the one-year range. Of immediate concern was the age group of 8 to 9 years of age, with 27% of this age group reporting having never spoken to parents about online safety. This is of concern since it is estimated that roughly 50% of this age group are regularly online and using some form of social media.

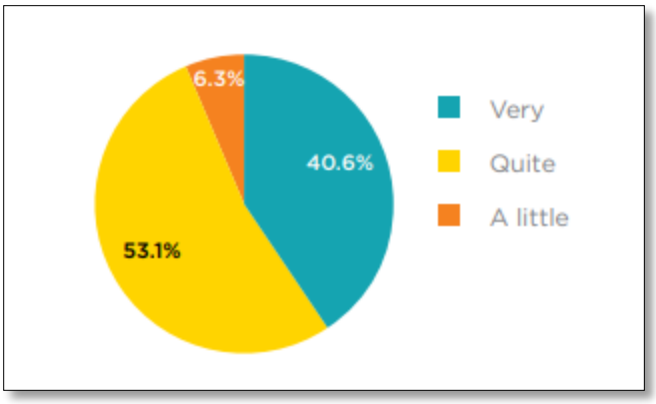


Table 7 Survey of parent's ability to implement CyberSafeIreland's recommendations from their information sessions. 2018 CyberSafeIreland annual report ***(Ibid) (Page 25 2018).***

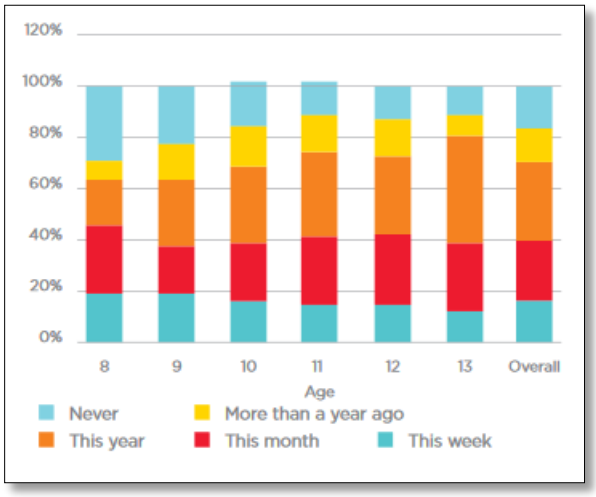


Table 8 Survey of parents whose children had spoken them about online safety by age. 2018 CyberSafeIreland annual report ***(Ibid) (page 24 2018).***

However, the survey was conducted over a total of 1,560 parents, with just less than 10% responding for a total of 145 parents. This we feel highlights that reach is important and there are many parents who are not yet accessing the information. While the benchmark of 10% of those responding is a respectable minimum benchmark.

Returning to the article in The Journal **(Ryan O. 2018)**, the report is referenced in, we can examine the views of the minister of education & skills, Richard Bruton TD on the matter of App safety among children. In 2017, the minister launched a new resource, in conjunction with WebWise.ie and An Garda Siochana called 'BeInCtrl' **(Webwise.ie 2019)** The blog is aimed at providing resources and developing policies to help both parents and Educators develop better safety practices with regard to on-line activity. The Taoiseach himself, Leo Varadkar TD, weighed in on the mater himself stating the following:

"We need to protect our children, that is always the most important thing, and protect them from predators who can now use the internet to get access to children.". – Leo Varadkar, TD

(Ryan O. 2018)

The report went on to state that a summit was due to be held which would include major stakeholders such as Gardai. Major tech companies and education providers. What we can take from this article and CyberSafeIreland's report, is that even as little as 1 year ago, the government was taking a very serious approach to the issue of online safety, as where Gardai, educators, Cyber Security watchdogs, and of course most importantly parents recognized this area as a very serious issue.

The report gives us our first indication of Which Apps we might cover. Snapchat remains the most popular App according to the report findings. 47% of children between 8 and 13 use Snapchat regularly. Instagram follows in second place with 36% of children using Instagram. In third place, the report finds that WhatsApp is also still popular among children with 33% of children using it. Being only one set of data points, we do not see this as enough data to determine which Apps we should investigate based of this alone and we shall pursue more data on this matter.

YouTube is covered as it proves to still be highly popular with both adults and children. Interestingly, CyberSafeIreland fund that many children are becoming YouTube content creators. The report also refers to a secondary YouTube App called YouTube Kids of those surveyed, 24% of participants had posted a video to YouTube. This is highlighted as an increase from the previous year of 13% showing a 50% growth rate in young content creation. 22% of children aged 9, and 25% of children of children aged 11 also reported posting videos.

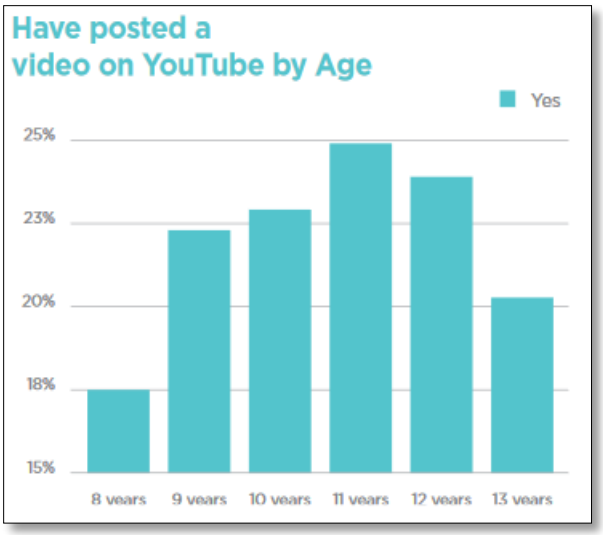


Table 9 Instances of young users of YouTube posting videos, by age. 2018 CyberSafeIreland annual report ***(Ibid) (page 22 2018).***

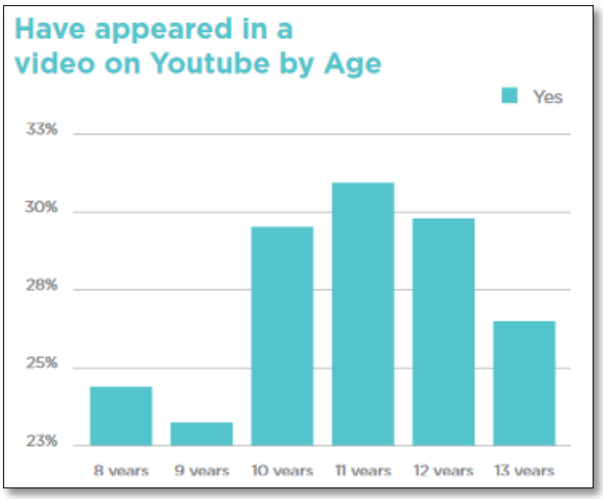


Table 10 Instances of young users of YouTube appearing in videos, by age. 2018 CyberSafeIreland annual report ***(Ibid) (page 22 2018).***

CyberSafeIreland states that YouTube has an age requirement of 13 to post videos showing that children or parents are unaware of the potential risks associated with youth and online App use, or the terms & conditions associated with YouTube. Yet again we see clear indications that more awareness is needed. Information needs to be more accessible, easier to understand and presented in a step by step useable platform. This report lends strong justification to our proposed service.

8.2: Custom Child App & Platform Use Survey

As our research is being carried out in the first quarterly period of 2019, this year's Annual report by CyberSafeIreland was at the time of researching, yet to be released. Therefore, to discern if the data was still relevant, we set out to design a custom survey.

Figure 04 Title of our survey as presented to student body of our university campus, conducted February 2019.

The survey was designed such that children or adults could respond and we sought to get both parents input and the input of our fellow student's siblings or close family relations. We did ask that the survey only be filled in by people living and working within Ireland. Our college has roughly 1000 students actively in attendance on a weekly basis, not counting part-time students and online courses as these students are generally far less likely to be involved in on campus activity and surveys. Aiming to match CyberSafeIreland's 10% response quota we issued the survey via mass email from our student's union.

We did ensure that our survey met all GDPR guidelines. We received 103 responses, meeting our minimum goal of approximately 10% participation giving us an acceptable sample group.

We had several questions we considered high priority and extremely pertinent regarding the process of selecting Apps to be investigated, which were as follows:

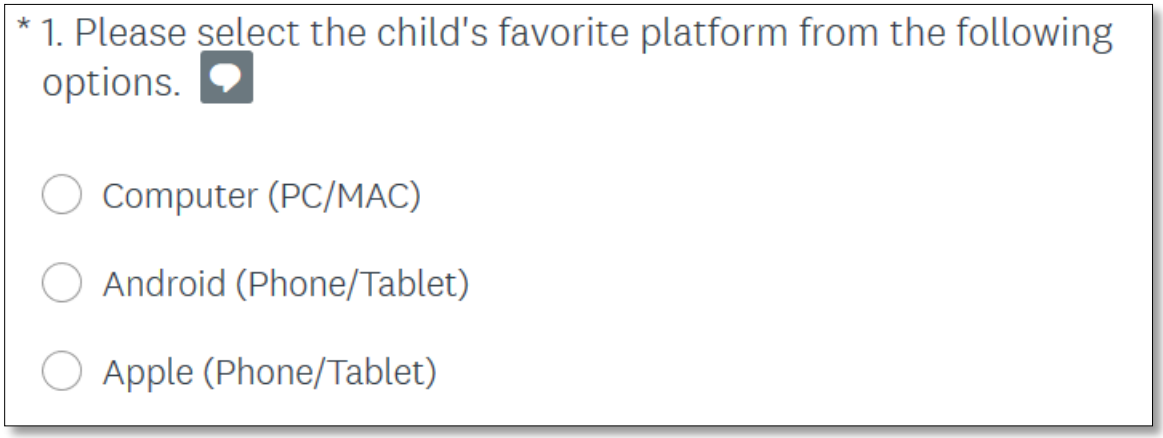


Figure 34 Question 1 our survey relating to platform use, conducted February 2019.

This question was aimed at narrowing our focus to which platforms we should be focusing on. We were interested to discover if children's online activity was focused in the mobile App market or if use of computers was popular among children. And if focused on mobile, which vendors.

Figure 35 Question 2 our survey in relation to age, conducted February 2019.

For this question, we wanted to determine the appropriate age groups into which our research would focus. The secondary purpose of this question was to reconfirm the previously examined data discovered in the CyberSafeIreland survey.

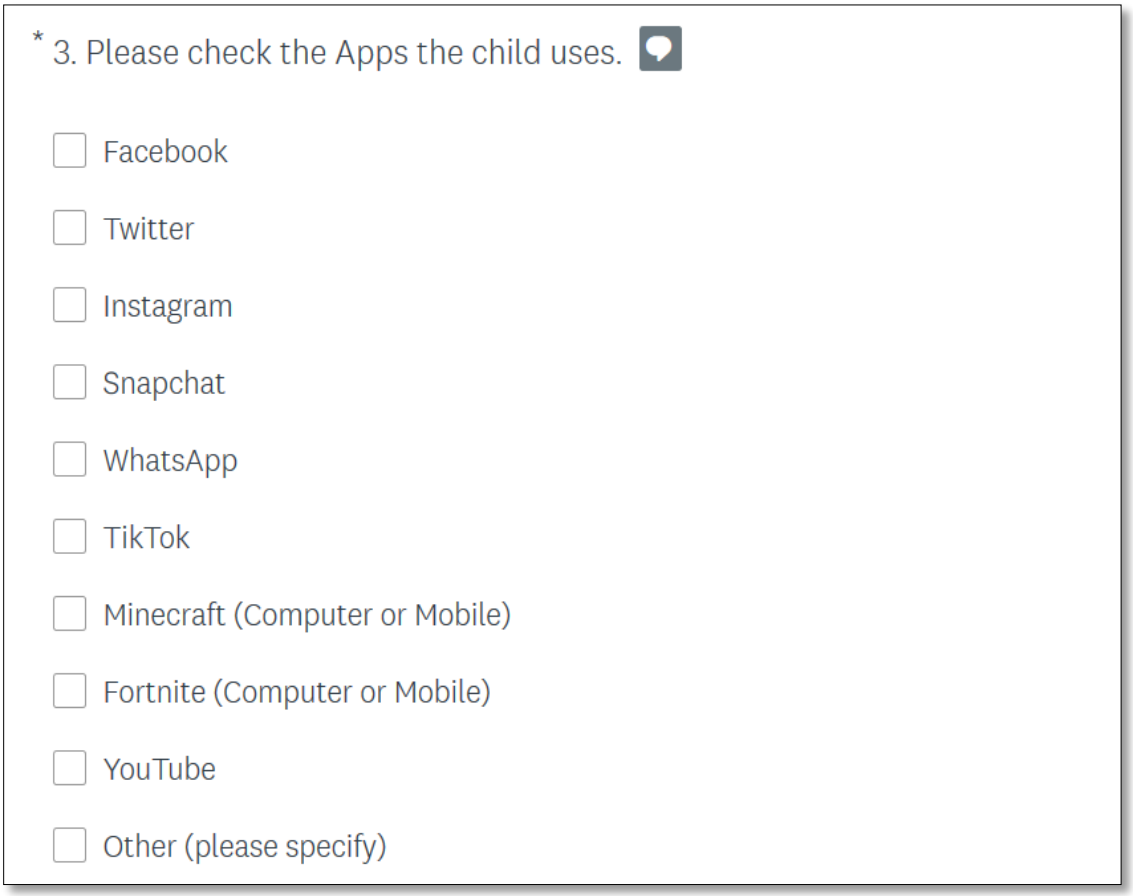


Figure 36 Question 3 of our survey relating to specific App use, conducted February 2019.

Question 3 focuses upon specific App use. This is the true beginning of our App selection process. Again, using the previous information discerned from CyberSafeIreland survey as a guideline, we seek to confirm if the popularity of the apps mentioned in their survey correlates with our data. If we wish to provide the most relevant and up to date data to children and parents, we must ensure that our data is accurate and consistent within the Irish market.

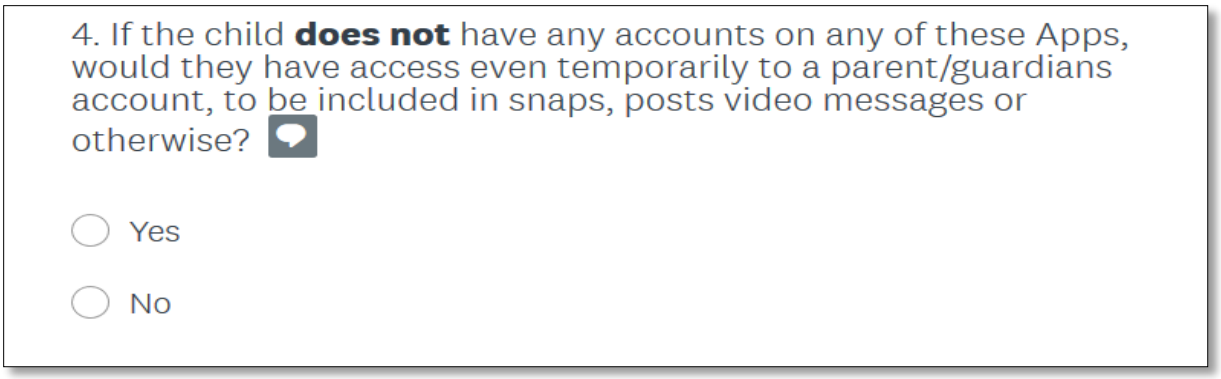


Figure 37 Question 4 of our survey in relation to online access, be it from personal or parent/supervisor accounts, conducted February 2019.

This question is aimed at determining if children firstly, have online access, and secondly, is it via parent or supervisor accounts or their own personal accounts. This will help us measure the degree of awareness and accountability in relation to child safety online.

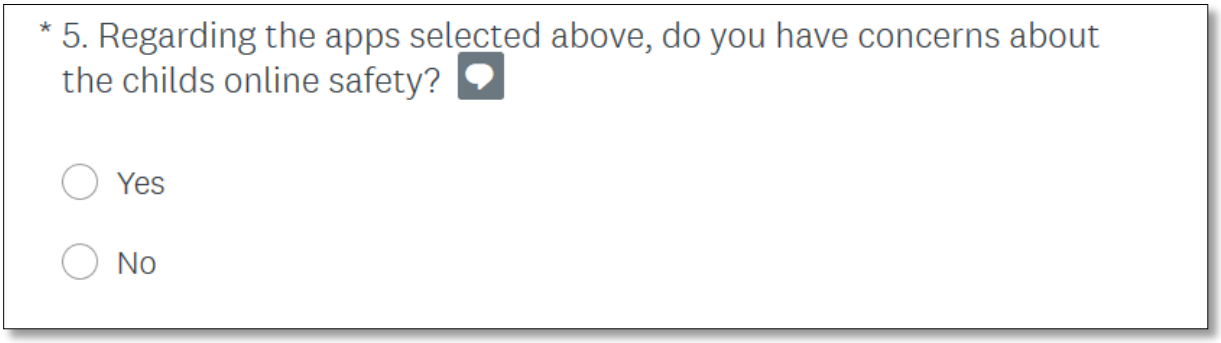


Figure 38 Question 5 aims at the level of awareness of parents regarding the risks of online access, conducted February 2019.

From this question, we aimed to expand upon our understanding of the level of awareness regarding the risks associated with online App use by children. This further serves to justify our projects focus.

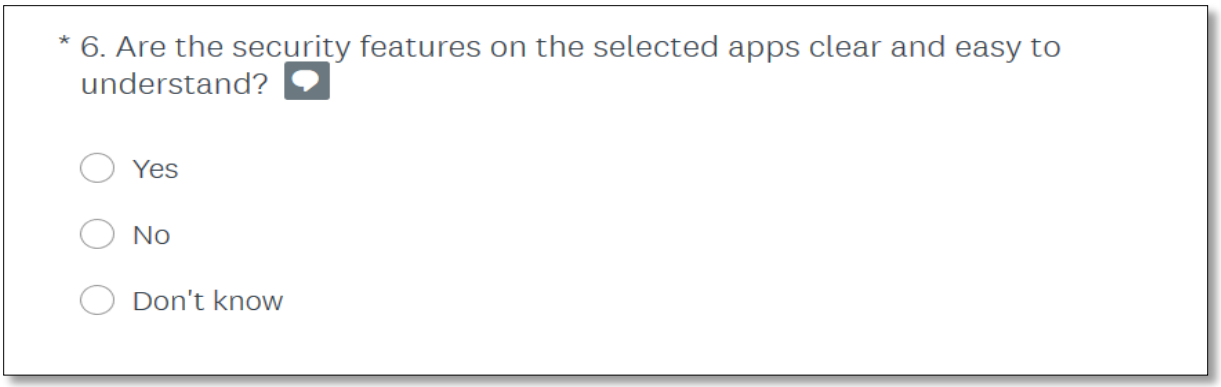


Figure 39 Question 6 is designed to discover the necessity for our need for our planned product (our blog), conducted February 2019.

This question is designed to establish the level of need for our planned blog. This will ultimately be a great consideration in the justification of our project.

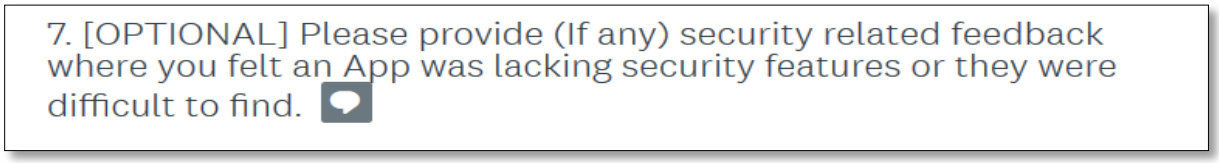


Figure 40 Question 7 allows for optional feedback from survey participants relating to security, conducted February 2019.

Question 7 serves to gather option feedback from survey participants. This is to establish if there are any areas we have overlooked, which are of relevance to our research.

8.3 Custom Child App & Platform Use Survey Results

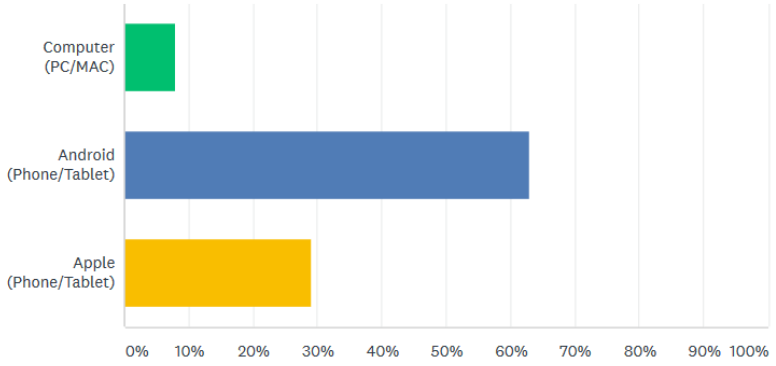
As previously mentioned we surveyed approximately 1000 students and we hoped for a 10% participation quota, giving us a goal of 100 responses. We were pleased to receive 103 responses.

RESPONDENTS: 103 of 103

Figure 41 number of survey respondents.

Please select the child's favorite platform from the following options.

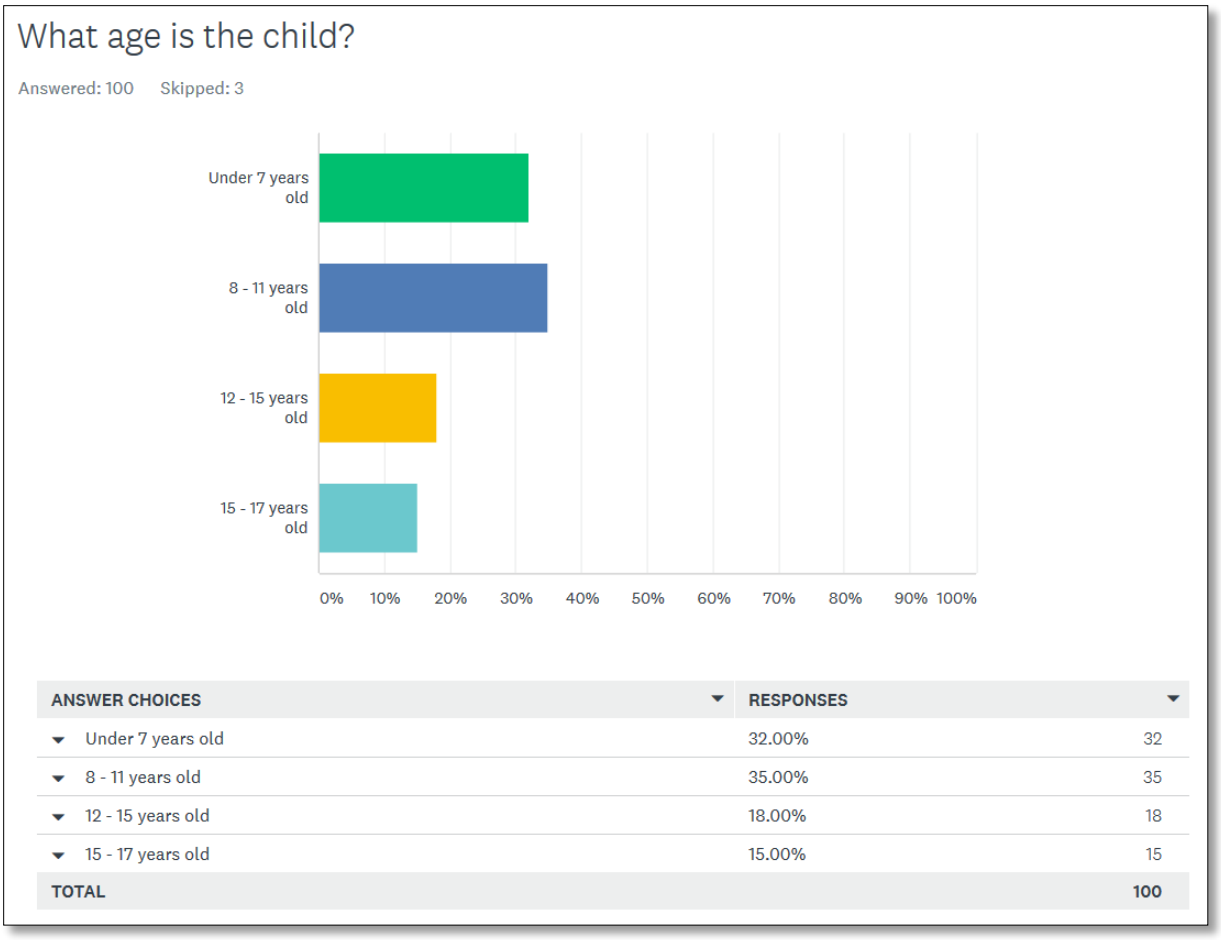
Answered: 100 Skipped: 3



ANSWER CHOICES	RESPONSES	
Computer (PC/MAC)	8.00%	8
Android (Phone/Tablet)	63.00%	63
Apple (Phone/Tablet)	29.00%	29
TOTAL		100

Table 11 Results of question pertaining to platform use, conducted February 2019.

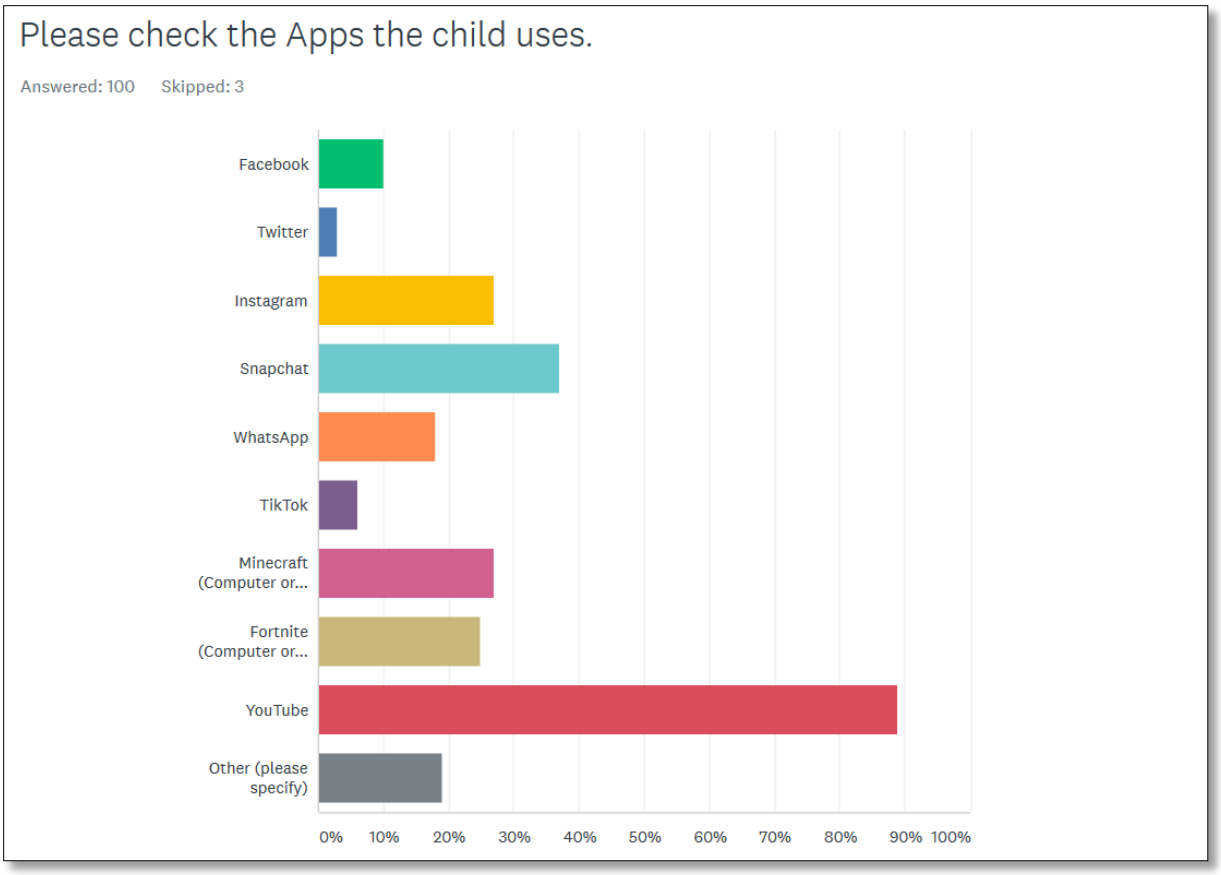
The results from question one highlight that the most popular platform is mobile with android taking the lead by roughly a 50% margin over Apple devices. Surprisingly desktop applications returned a result of only 8% virtually eliminating this for the focal point of our research. Unsurprisingly Android takes a large share of the market, however, we did not anticipate such a large lead over apple devices, with Android returning 63% usage and Apple returning 29% usage. This tells us not only can we narrow our focus to the mobile platform market, but we should focus on the Android platform. We do not anticipate that many features would differ from android to apple devices and similarly, we would expect the same feature set regarding settings.



ANSWER CHOICES	RESPONSES	
Under 7 years old	32.00%	32
8 - 11 years old	35.00%	35
12 - 15 years old	18.00%	18
15 - 17 years old	15.00%	15
TOTAL		100

Table 12 Results pertaining to the age of the child in question, conducted February 2019.

Alarmingly we see a surprising trend highlighting that the two largest age groups containing children under 7 years old and children aged 8 – 11 years old. While we did anticipate young users, the results for children under 7 years old at 32%, was far greater than expected. While the 35% pertaining to 8-11-year olds were about what we expected having closely examined CyberSafeIreland's result sets. One last surprise was returned from this question in that the older groups 12-15 and 15-17 returned a surprisingly low level of usage according to our data. While the variances between the younger and older age groups are surprising, we feel the younger age groups alone are a reasonable justification while both groups together are tantamount to a significant justification.



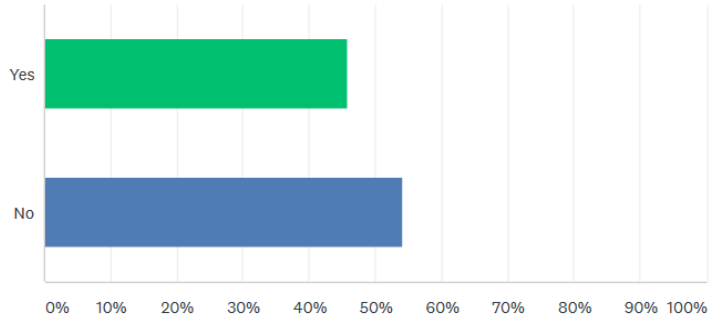
ANSWER CHOICES		RESPONSES	
YouTube		89.00%	89
Snapchat		37.00%	37
Instagram		27.00%	27
Minecraft (Computer or Mobile)		27.00%	27
Fortnite (Computer or Mobile)		25.00%	25
Other (please specify)	Responses	19.00%	19
WhatsApp		18.00%	18
Facebook		10.00%	10
TikTok		6.00%	6
Twitter		3.00%	3
Total Respondents: 100			

Table 13 Results pertaining to the Apps the child uses, conducted February 2019.

This question returns a surprising result with YouTube leaps and bounds ahead of the curve in terms of popularity at 89% acknowledging regular use. After YouTube is snapchat at 37% usage followed by Minecraft and Instagram tied with 27% usage. Fortnite comes next with 25% of usage. After that we allowed participants to enter an App that is not listed here however we did not find a trend among the responses. After this WhatsApp comes next with 18% of usage, followed by Facebook at a surprising 10% usage. Next is TikTok at 6% followed by Twitter at 3%.

If the child does not have any accounts on any of these Apps, would they have access even temporarily to a parent/guardians account, to be included in snaps, posts video messages or otherwise?

Answered: 83 Skipped: 20



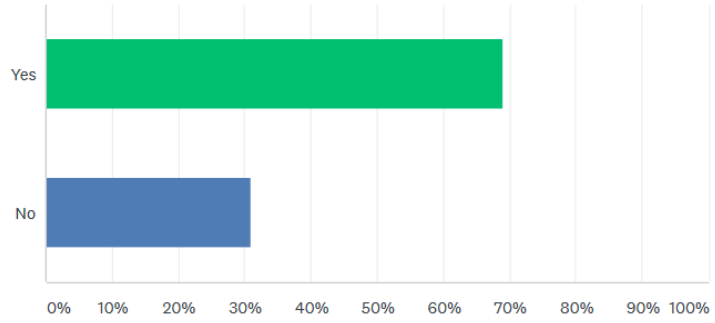
ANSWER CHOICES	RESPONSES	
Yes	45.78%	38
No	54.22%	45
TOTAL		83

Table 14 Results pertaining to parents or supervisors providing online access to children who don't have their own device, conducted February 2019.

The results displayed here shows us that 45.78% of parents or supervisors would allow their children to access their account temporarily to be included in snaps, post video messages or otherwise. 54.22% of guardians wouldn't allow this however.

Regarding the apps selected above, do you have concerns about the childs online safety?

Answered: 100 Skipped: 3



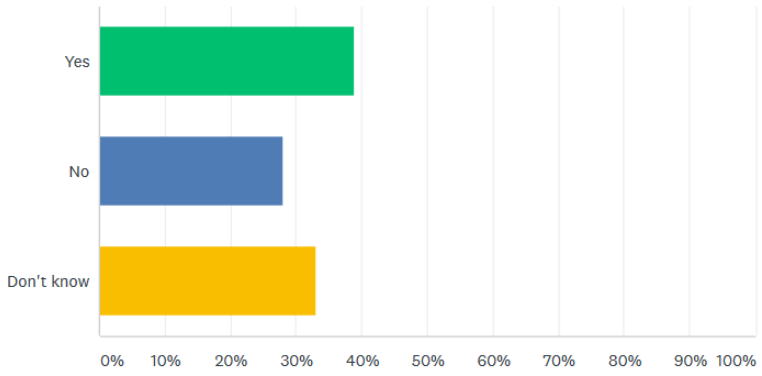
ANSWER CHOICES	RESPONSES	
Yes	69.00%	69
No	31.00%	31
TOTAL		100

Table 15 Results pertaining to concerns about online safety, conducted February 2019.

From the results shown above, we can see that 69% of supervisors are concerned about the child's online safety. Despite this, it is still worrying that 31% of parents or supervisors are not concerned about the child in questions online safety.

Are the security features on the selected apps clear and easy to understand?

Answered: 100 Skipped: 3



ANSWER CHOICES	RESPONSES	
Yes	39.00%	39
No	28.00%	28
Don't know	33.00%	33
TOTAL		100

Table 16 Results pertaining to how parents or supervisors understand security features on selected Apps, conducted February 2019.

As you can see from the results above, only 39% of parents or supervisors felt that the security features of the Apps the child in question used were clear and easy to understand. This left 28% of parents or supervisors feeling they weren't easy to understand and 33% not knowing about the security features. What we see from this is that over 50% of survey participants show that either features were hard to find or understand yet again we feel that this lends further weight to the justification of our project.

[OPTIONAL] Please provide (If any) security related feedback where you felt an App was lacking security features or they were difficult to find.

Answered: 19 Skipped: 84

Figure 42 Finally, an Optional text box for participants to provide security related feedback for Apps

We scrutinized these answers to review relevant data points insuring to include points that contradicted our project justification. We did not document what we felt to be irrelevant answers.

I was sent a WhatsApp message yesterday of the woman beheaded on the M50 car crash. It was only by pure luck that my 9-year-old son was not the one who opened it. Totally unsatisfactory security. Should be easrier to bar parts of my phone from access

1/25/2019 11:28 AM View respondent's answers Add tags

Figure 43 Optional Response 1 from our custom Child App & Platform Use Survey, conducted February 2019.

What we see from our first response is a parent who received an inappropriate message via WhatsApp. The parent goes on to suggest that the App lacks security features however what we find is a lack of understanding of proper device security procedures. All devices come with the ability to lock a screen using a passcode or unlock pattern and should be utilized to prevent unauthorized access to the phone by children.

Pre loaded Parental mointoring software should be standard on android and apple devices and allow remote anonymous access from a parents computer.

1/24/2019 4:56 PM View respondent's answers Add tags

Figure 44 Optional Response 2 from our custom Child App & Platform Use Survey, conducted February 2019.

Here, a parent informs us of their desire to see parental monitoring software preinstalled on every device. This was a fascinating response which lead us to begin to question whether we should include a review of security-based Apps themselves.

kids are quite young (6 & 3 year old), they can quickly navigate to and view perhaps unsuitable content on you tube which may not be inappropriate to older children. maybe different levels of filtering required

1/24/2019 4:04 PM View respondent's answers Add tags

Figure 45 Option Response 3 from our custom Child App & Platform Use Survey, conducted February 2019.

As we can see above the respondent is unhappy with the ease of access with which their children, who are of a very young age, can access YouTube content. While we take this point on board we cannot ignore the fact that yet again a parent has allowed unfiltered access to an unsecure device.

It didn't require the childs age and it meant the child could access video content that wasn't age appropriate

1/24/2019 2:55 PM View respondent's answers Add tags ▾

Figure 46 Optional Response 4 from our custom Child App & Platform Use Survey, conducted February 2019.

Yet again another respondent when referring to YouTube is unhappy with the ease of access to age restricted content.

I dont think any child should have unsupervised access to most of those apps. Im not sure about their child security features but as a parent I probably would would be very critical of them.

1/24/2019 1:43 PM View respondent's answers Add tags ▾

Figure 47 Optional Response 5 from our custom Child App & Platform Use Survey, conducted February 2019.

Here a parent supports our presupposition that children should not have unsupervised access to Apps.

When installed a number of the apps are completely open and allow everything. The default position should be to deny everything!

1/24/2019 11:47 AM View respondent's answers Add tags ▾

Figure 48 Optional Response 6 from our custom Child App & Platform Use Survey, conducted February 2019.

This response is rather vague; however, we feel the respondent is drawing attention to the fact that any App can be installed, and no parental features exist to prohibit installation of Apps by default. This an excellent point. And yet again, we are forced to consider the possibility of covering at least 1 security App which would provide this functionality.

Marketing is what we tend to see in the app documentation, which is a very view point than the engineers that wrote the apps. My kids (2 under 12) use our phones occasionally and know the concern we have about online hooks that appear in the apps, buy tokens/ post to facebook, have to watch the video ads and know we do not allow them to acknowledge or submit without asking. The nature of the apps after a submit is to torment the phone owner with pop-ups which generally earns the kids a block on mobile device access for 6 weeks.

1/24/2019 10:49 AM View respondent's answers Add tags

Figure 49 Optional Response 7 from our custom Child App & Platform Use Survey, conducted February 2019.

Here we see an interesting response from a parent showing reasonable understanding of the risks and pitfalls regarding marketing campaigns embedded into online based Apps. This respondent has even gone so far to prepare a set of rules regarding what their child may or may not interact with as well as a disciplinary procedure should click on content they are prohibited from. While we are impressed by this, we also feel more could be done to restrict the child without the need to punish for what may be genuine mistakes. However, this feedback was greatly appreciated.

Snapchat maps uploads your location unless you go out of your way to turn it off. When a child first creates their account they dont always realise how exact the GPS is and how easily someone could find them.

1/24/2019 10:49 AM View respondent's answers Add tags

Figure 50 Optional Response 8 from our custom Child App & Platform Use Survey, conducted February 2019.

As we can see here, we have a concerned response regarding Snapchat's geolocation tracking. What the user is highlighting here is that when a child creates an account on Snapchat they may be unaware of the potential danger of using Snapchat's geolocation. This presents us with another interesting view point which suggests we should research snapchat.

You tube has age restrictions on videos but i feel that the ads shown in between the videos are not appropriate for the age of the children watching the videos. Also some of the games get these kind of ads in between. There is no way to block them.

1/24/2019 10:39 AM View respondent's answers Add tags

Figure 51 Optional Response 9 from our custom Child App & Platform Use Survey, conducted February 2019.

What we see here is that another respondent highlights concerns surrounding the availability of both content and advertisements on YouTube. We are seeing a trend which points to YouTube being a real

area of concern for parents. Strong consideration must be given to carrying out in depth research into YouTube to address these concerns.

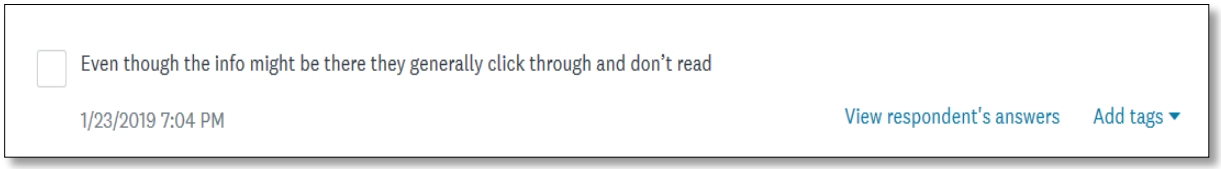


Figure 52 Optional Response 10 from our custom Child App & Platform Use Survey, conducted February 2019.

Here we can see that a respondent shows concern that parents, or supervisors, may be skipping through terms & conditions and not reading them which could hold information regarding safety.

Figure 53 Optional Response 11 from our custom Child App & Platform Use Survey, conducted February 2019.

Here we have another respondent adding weight to the statistics investigated previously which suggests we should include Snapchat and Instagram in our research.

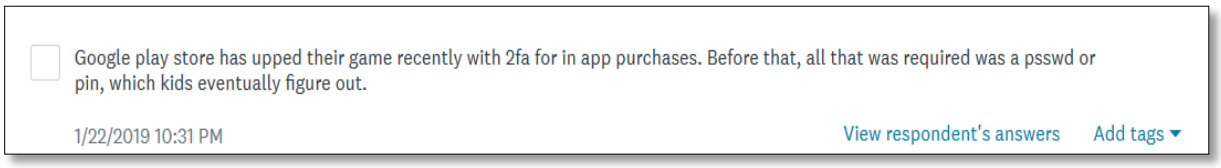


Figure 54 Optional Response 12 from our custom Child App & Platform Use Survey, conducted February 2019.

Here we have a response that is slightly contrary to our presupposition. The respondent suggests that Google have recently increased security via two-factor authentications. The user indicates that prior to this increase in security, access was easier to gain via password. We certainly feel that two-factor authentication is a security feature that should be included more in Apps.

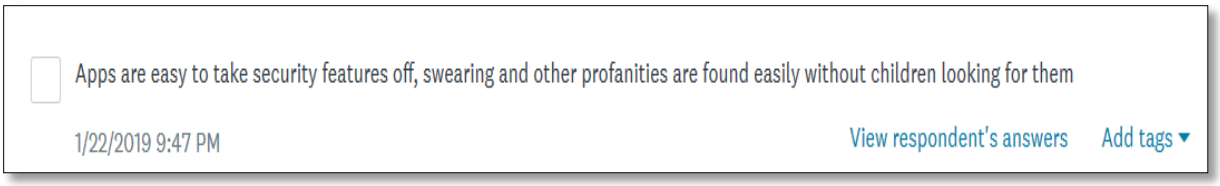


Figure 55 Optional Response 13 from our custom Child App & Platform Use Survey, conducted February 2019.

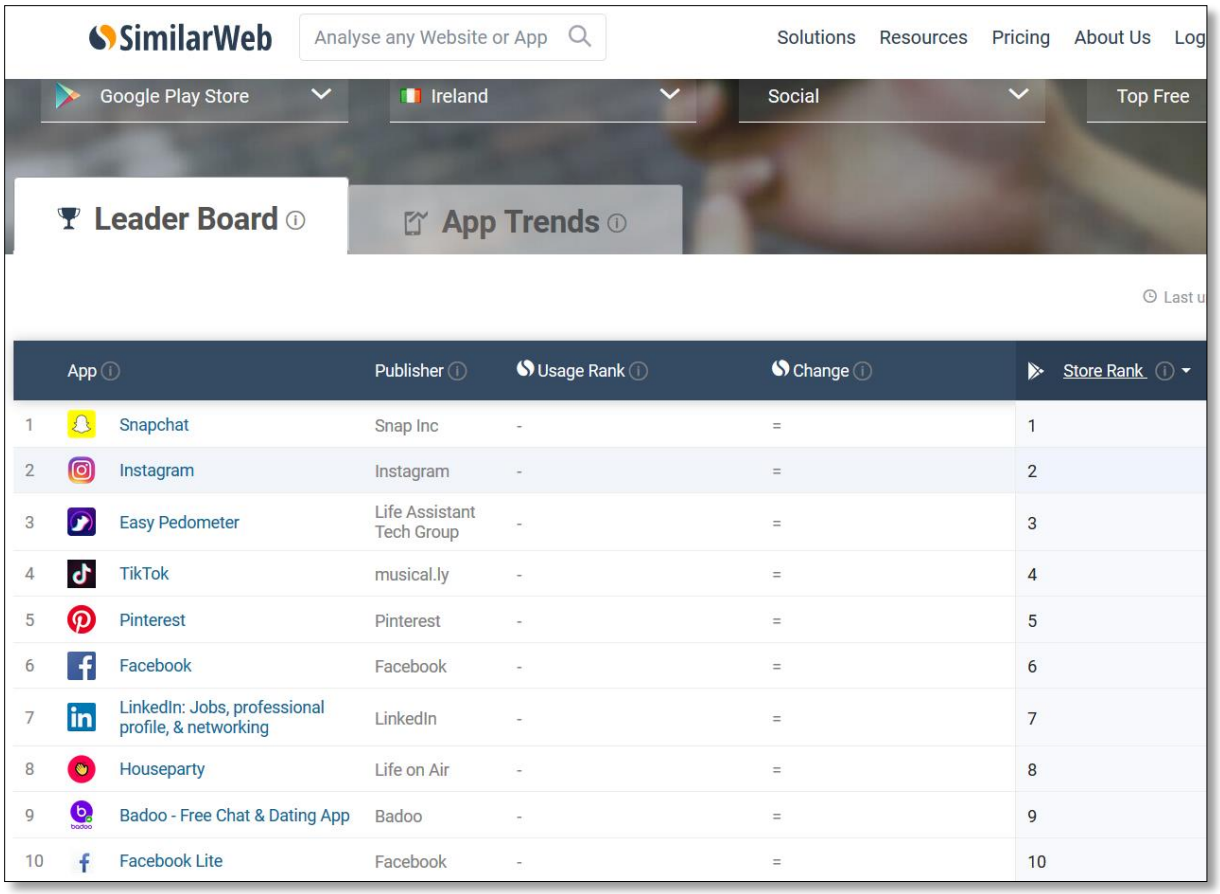
In this response, the respondent is suggesting that while security features may exist the might be too easy to remove. Profanity can be easily found without children even seeking it. This suggests that users may appreciate a feature or App which may prevent settings inadvertently being changed. We will attempt where possible to highlight these features in any Apps we investigate.

8.4 Google Play Store / Apple Store

As a third data set to help us narrow the selection process for the Apps we shall research, we analysed data pertaining to the App stores. As we have narrowed our focus to the mobile market, we shall examine the Google Android store, and the Apple store to see if most popular Apps corelate with our previous data sets.

To view this data, we used the website SimilarWeb **(SimilarWeb 2019)** which is plugged directly into The Google developer API. This produces fantastic results which can be broken down by store, region App type and more. We were able to discern patterns in popularity across both platforms. With Android device popularity exceeding that of Apple devices, we will allow android devices statistics to supersede those of Apple, should we deem it necessary.

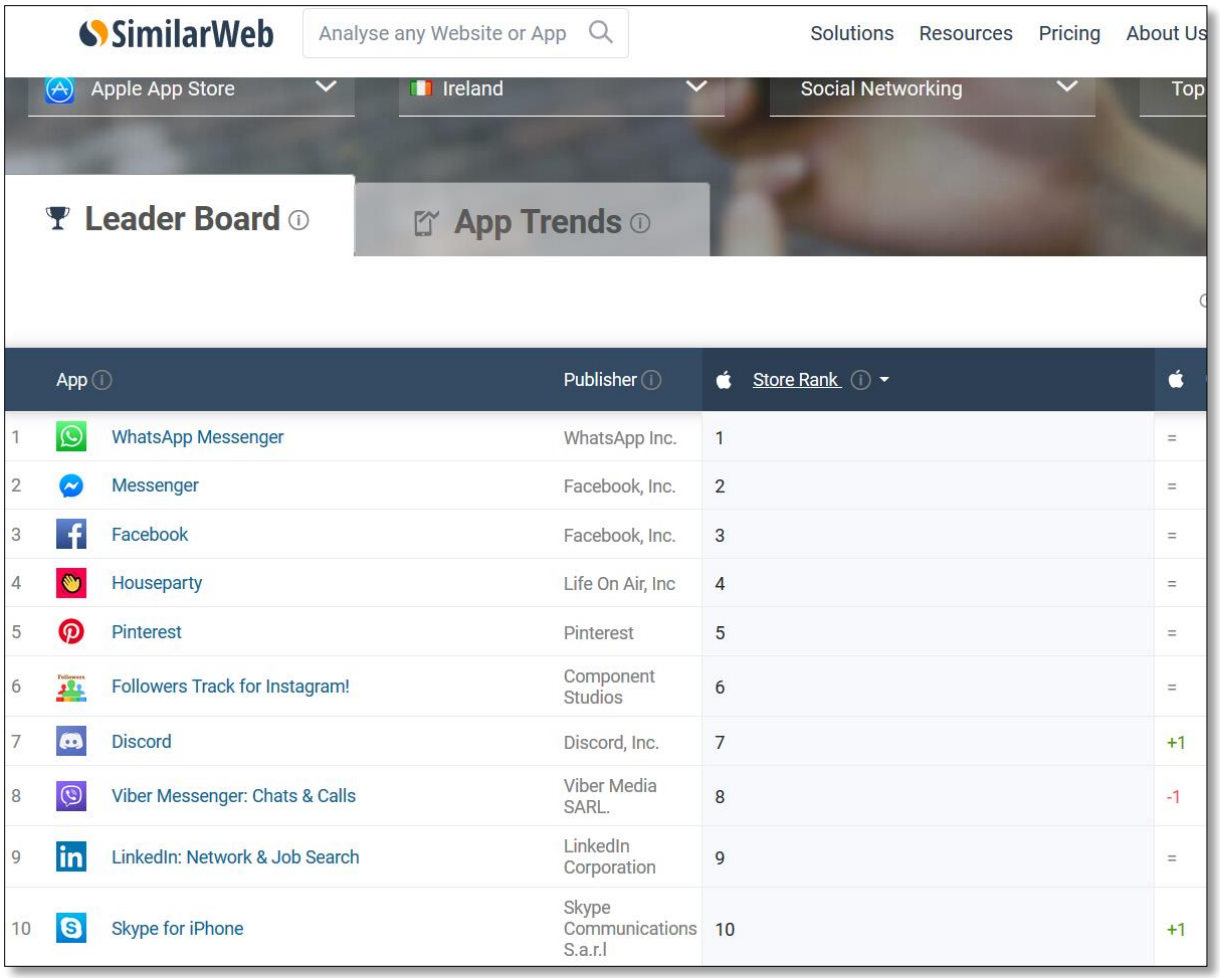
Lastly, before we examine the results, it should be noted that Most of the main Google Apps such as YouTube come pre-installed and may therefore not be listed among the results. The last factor to be considered is that Apps are not broken down by age groups.



	App	Publisher	Usage Rank	Change	Store Rank
1	Snapchat	Snap Inc	-	=	1
2	Instagram	Instagram	-	=	2
3	Easy Pedometer	Life Assistant Tech Group	-	=	3
4	TikTok	musical.ly	-	=	4
5	Pinterest	Pinterest	-	=	5
6	Facebook	Facebook	-	=	6
7	LinkedIn: Jobs, professional profile, & networking	LinkedIn	-	=	7
8	Houseparty	Life on Air	-	=	8
9	Badoo - Free Chat & Dating App	Badoo	-	=	9
10	Facebook Lite	Facebook	-	=	10

Table 17 Results from Google Play store, Ireland, Social App Type ***(SimilarWeb 2019) [Accessed March 2019].***

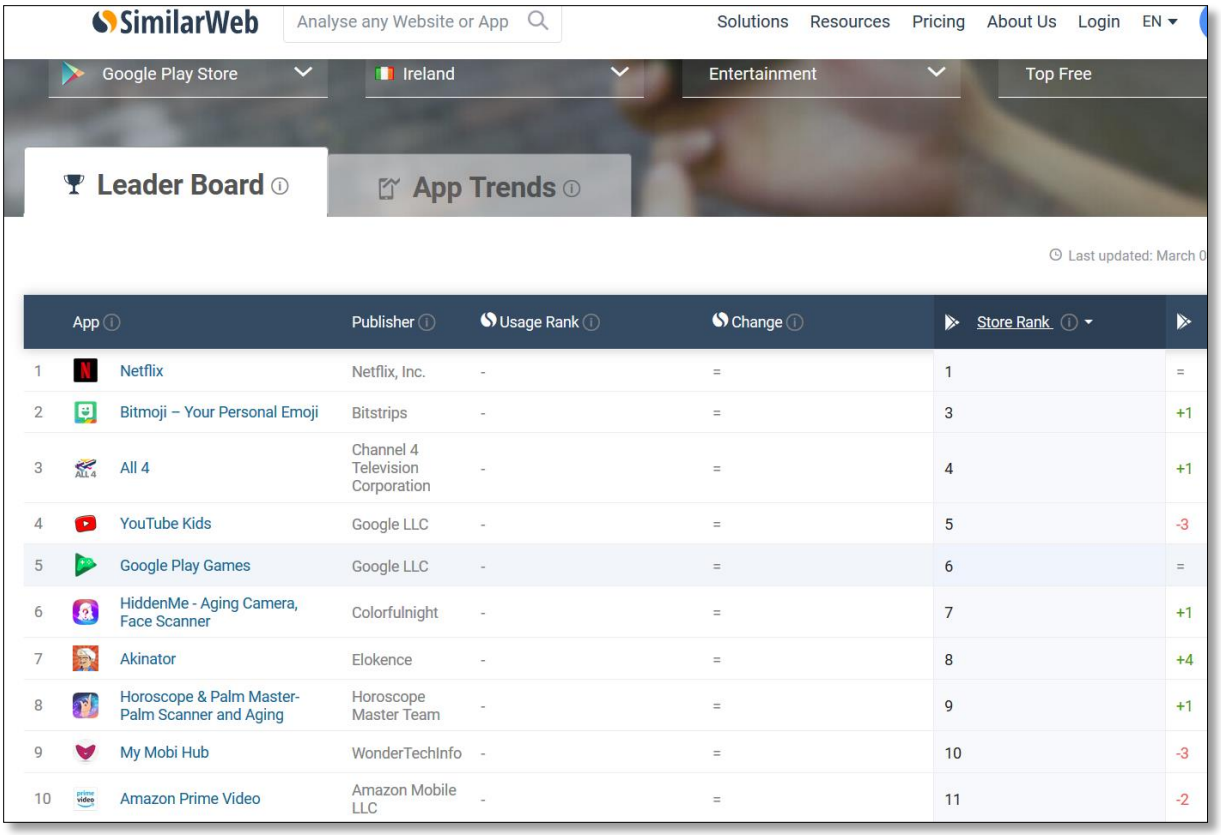
Above, we can see that among the sub group of social Apps Snapchat, Instagram both rate high on the google android store alongside Kik.



	App	Publisher	Store Rank	
1	WhatsApp Messenger	WhatsApp Inc.	1	=
2	Messenger	Facebook, Inc.	2	=
3	Facebook	Facebook, Inc.	3	=
4	Houseparty	Life On Air, Inc	4	=
5	Pinterest	Pinterest	5	=
6	Followers Track for Instagram!	Component Studios	6	=
7	Discord	Discord, Inc.	7	+1
8	Viber Messenger: Chats & Calls	Viber Media SARL.	8	-1
9	LinkedIn: Network & Job Search	LinkedIn Corporation	9	=
10	Skype for iPhone	Skype Communications S.a.r.l	10	+1

Table 18 Results from the Apple store, Ireland, Social App Type ***(Ibid 2019) [Accessed March 2019]****.*

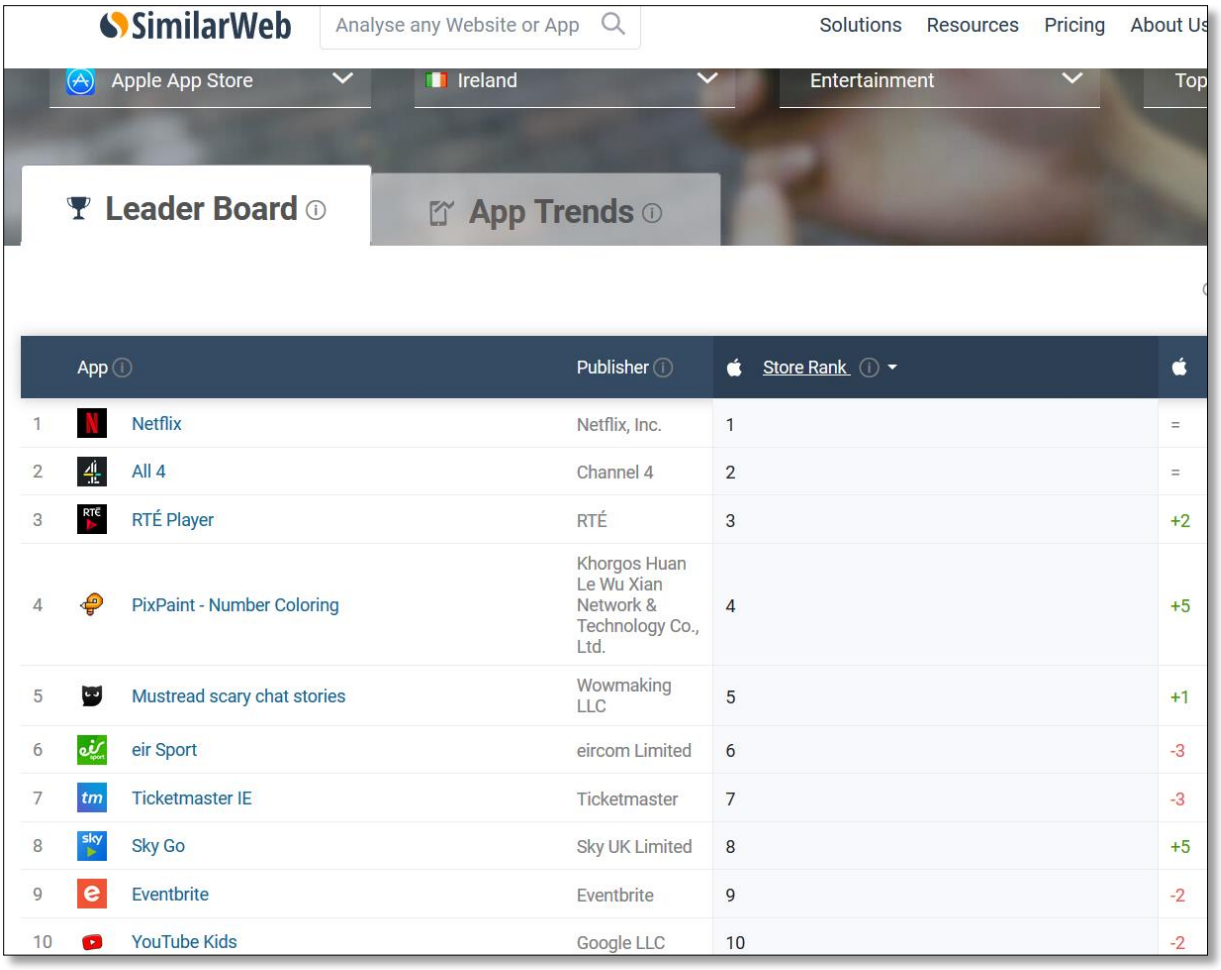
The results from the Apple Store present a slightly different picture. With WhatsApp topping the charts. Messenger and Facebook take up the second and third place. We do some correlation here with our previous data point where WhatsApp is concerned. However, our previous data sets suggest neither Facebook or Messenger are popular amongst younger users in the mobile market. While certainly not conclusive, this is indicative of Apple devices being more popular with adult users. The higher price point of Apple device would certainly support this.



	App	Publisher	Usage Rank	Change	Store Rank	
1	Netflix	Netflix, Inc.	-	=	1	=
2	Bitmoji – Your Personal Emoji	Bitstrips	-	=	3	+1
3	All 4	Channel 4 Television Corporation	-	=	4	+1
4	YouTube Kids	Google LLC	-	=	5	-3
5	Google Play Games	Google LLC	-	=	6	=
6	HiddenMe - Aging Camera, Face Scanner	Colorfulnight	-	=	7	+1
7	Akinator	Elokence	-	=	8	+4
8	Horoscope & Palm Master-Palm Scanner and Aging	Horoscope Master Team	-	=	9	+1
9	My Mobi Hub	WonderTechInfo	-	=	10	-3
10	Amazon Prime Video	Amazon Mobile LLC	-	=	11	-2

Table 19 Results from Android store, Ireland, Entertainment App Type ***(SimilarWeb 2019) [Accessed March 2019]****.*

Here, we see the results from the Android store, entertainment App type. Interestingly, while we would not expect to see YouTube here, being as that it is preinstalled on most popular devices, we do see YouTube Kids making an appearance, which does not come pre-installed. The fact that a secondary YouTube App makes the cut speaks volumes as to the popularity of the parent App.



	App	Publisher	Store Rank	
1	Netflix	Netflix, Inc.	1	=
2	All 4	Channel 4	2	=
3	RTÉ Player	RTÉ	3	+2
4	PixPaint - Number Coloring	Khorgos Huan Le Wu Xian Network & Technology Co., Ltd.	4	+5
5	Mustread scary chat stories	Wowmaking LLC	5	+1
6	eir Sport	eircom Limited	6	-3
7	Ticketmaster IE	Ticketmaster	7	-3
8	Sky Go	Sky UK Limited	8	+5
9	Eventbrite	Eventbrite	9	-2
10	YouTube Kids	Google LLC	10	-2

Table 20 Result from the Apple Store, Ireland, Entertainment App Type ***(SimilarWeb 2019) [Accessed March 2019]****.*

Here we see a lack of correlation on the Apple Store, when we view the entertainment App Type. What this evidence again suggests, is that Apple devices may simply be more popular with Adults. Given that Apple devices tend to be more expensive, and thus less accessible for children.

8.5 App Selection

Our first data set, the CyberSafeIreland 2018 **(CyberSafeIreland 2018)** annual survey strongly indicates via its statistics that the Apps we should cover are as follows:

- Snapchat
- WhatsApp
- YouTube
- Instagram

Our seconds data set, our custom Child App & Platform Use Survey 2018 strongly indicates via its statistics that the Apps we should cover are as follows:

- YouTube
- Snapchat
- Instagram
- WhatsApp

Our third data set, statistics pertaining to App stores, suggests we should cover these Apps.

Android:

- Snapchat
- Instagram
- Netflix
- Bitmoji

Apple:

- WhatsApp
- Messenger
- Netflix
- All 4

As previously mentioned YouTube is pre-installed on most devices, therefore, it's not displayed in any of the App Store result sets. Furthermore, the App Store results are not broken down by age.

Finally, our survey datasets show us that Apple devices are not as popular as Android devices among children. Having taken these points on board we feel we can comfortably discard the Apple store data, even though one datapoint corelates with our other two data sets. This data point tells us at the very least, in covering WhatsApp, it would be relevant to some adults.

Examining the Android results we saw a direct correlation between two datapoints in all three of our datasets. Therefore, the decision that the Android results supersede the Apple store results and hold more relevance to the decision-making process is felt to be justified. We have decided that the first two Apps to be covered will be Snapchat and Instagram.

Returning to our previous two datasets, we see that from these two datasets, YouTube is both popular and of primary concern to parents. Therefore, YouTube will be included in our research.
Lastly, we again see correlation between our other two datasets which shows WhatsApp as one of the more popular Apps, it should take its place as the fourth App we will research.

As laid out in our project scope we have set out to cover a minimum of three Apps and a maximum of five. With four Apps now selected, we shall reserve the fifth slot for any App which we may encounter during our research that is deemed to provide a level of increased security such that it cannot be ignored. Therefore, we can consider the App selection complete without Apps being the following:

- Snapchat
- Instagram
- WhatsApp
- YouTube

8.6 Risk Relating to Unfiltered Online Access

8.6.1 Predators & Grooming

This is a very sensitive subject, and as such must be handled delicately. We must weigh the dangers associated with this kind of malicious online user, and the devastating results of their online interactions with children, against the potential harm any story we may report on might have on those who come to our blog to learn.

We recognise that having to relive a trauma that a user, or their child have gone through can have a huge impact, however we must highlight some of the risks involved with unfiltered online activity. We shall therefore, attempt to use online incidents where victims are not named, and the cases have a sweeping scope and impact.

Two specific cases have been pre-selected which we feel highlight the risks posed to all age groups regarding both grooming, and the availability of personal images and content due to data sharing restrictions and precautions not being employed.

8.6.1.1 Case 1

In his article entitled 'Ten per cent of online child sex abuse images feature infants' Conor Gallagher reports, 6th February 2018, for The Irish Times online **(Gallagher C. 2018)**, that one on every ten online child abuse images detected in Ireland depicts children under 3 years of age. A statistic we feel will be shocking to most parents.

The article goes on to discuss how Hotline.ie received 7,141 tip offs about suspected child abuse imagery. Most of the cases that were reported, were by people who simply stumbled across this type of imagery showing that it is widely and publicly accessible. The former senator and child protection advocate, Jillian van Turnhout is quoted as saying:

> *"People think of the victims as being teenagers and upwards. There is no age too young for these images. Europol has dealt with images with an umbilical cord". - Jillian van Turnhout*
>
> ***(Gallagher C. 2018)***

The article goes on to breakdown confirmed online child abuse material reported to hotline as follows: 10% fell into age group 3 years or younger, 61% fell into the age group 4-12 years of age, and 29% fell into the age group 13-16 years old. However, hotline recently updated their data set which highlights, and even more worrying set of statistics as seen below.

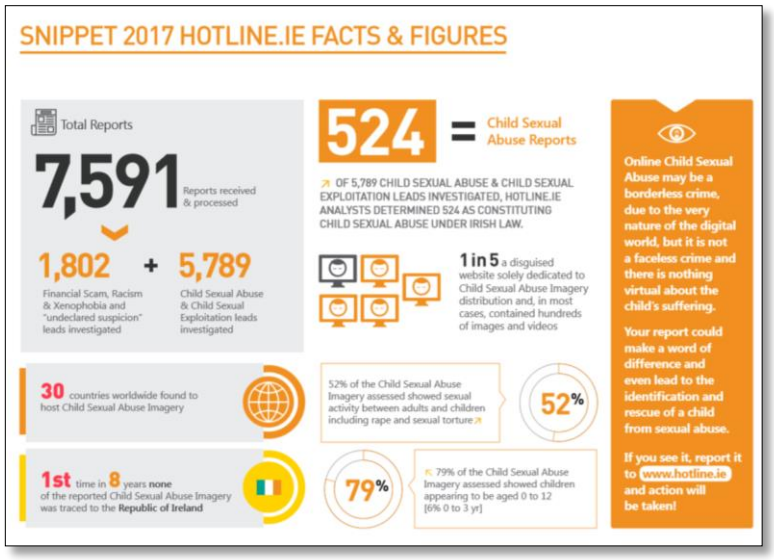


Figure 56 Chart from the 2017 Hotline.ie Annual Report ***(Hotline.ie) [Accessed March 2019]***

The above chart, taken from the 2017 Hotline.ie annual report **(Hotline.ie Annual Report)**, details that out of 7,591 cases reported to Hotline, 5,789 constituted child sexual abuse or exploitation investigations. 30 countries worldwide where confirmed as finding child sexual imagery hosted online. These latest figures reveal that for the first time in 8 years, none of the hosted material was traced back to Ireland. 1 out of 8 years! A very worrying data point indeed.

1 in 5 of the websites investigated by Hotline.ie where revealed to be disguised websites solely designed to distribute Child Sexual Abuse Imagery. Of the sexual abuse imagery investigated, 53% appeared to depict rape and sexual torture and 79% appeared to depict children as young as new-borns, and as old as 12. These are truly horrific statistics.

There are two very important things that should be obvious here, which the report does not mention but which we feel should be taken from these figures. Firstly, a demand for such despicable content exists, and secondly, that demand is being met. Therefore, ensuring a reduced visibility of children's content and accounts online is fully justified and demanded.

Lastly this article serves to further support the findings of the 2018 CyberSafeIreland annual report, that all age groups of children are exposed to these risks.

On the very same day as our previous article was published another article was published, once again online for the Irish Times, this time by Conor Lally, 6th February 2018, entitled 'Gardaí find 70,000 child sex images on man's computers', reports that Gardai had discovered 70,000 images of child sexual abuse on computers alleged to belong to a man targeted in a series of raids **(Lally C. 2019)**. The raids were conducted over a wide range of counties including, Dublin, Meath, Wicklow, Wexford, Carlow-Kilkenny, Laois, Kerry, Waterford and Kildare. The operation which was coordinated with international agencies including the FBI's child exploitation unit and law enforcement agencies in Canada was codenamed Operation Ketch III **(An Garda Síochána 2018)** and Gardai estimated that along with the 70,000 images unrecovered, up to 150,000 images went unrecovered.

This report reveals that Irelands Child sex abuse problem is part of the larger international problem and the scope of the problem is wide ranging, reaching relatively quiet and sparsely populated counties, respectively, when compared to large, densely populated counties such as Dublin. This confirms the problem is national, not localized and if there was any doubt of the dangers of online grooming they are surely laid to rest by these two articles alone. However, sadly, as anybody who has dared to investigate this subject material can attest to, this is unfortunately just the tip of the ice berg.

8.6.1.2 Case 2

Now we shall examine a particularly sensitive case. The case relates to the grooming of a 14-year-old girl by a Canadian national named Joshua Robert Tremblay. We shall not name nor touch on any personal specifics pertaining to the victim in this case for obvious reasons, but Mr. Tremblay has since been tried and convicted.

As reported by Anne Lucey, 13th April 2017 and updated April 20th, 2017 ***(Lucey A. 2017)***, online, once again for The Irish Times; in her article entitled 'Canadian who travelled to Ireland for sex with girl (14) sentenced'. Mr Tremblay was found to have contacted the young victim through social media. Canadian police, having investigated the case found that not only had the man sent nude pictures of himself to the victim, but he had travelled to Ireland and had intimate relations with the child on several occasions.

The specifics of this case are truly horrifying and even just investigating the story proved very difficult for our group. In this case, the perpetrator managed to successfully manipulate the young victim into agreeing to have intimate relations with him. Luckily this did not affect the Canadian Crowne Prosecution Service from trying the accused. This case was so reprehensible in the eyes of both Irish Gardai and Canadian police, that though no specific treaty exists which forces Canadian police to co-operate with Irish Gardai, laws do exist that allow Canadian Authorities to try a Canadian citizen at home for sex crimes committed in foreign states; and in this case the Canadian police forces co-operated to the fullest of their extent. They ultimately did succeed in securing a conviction against Mr. Tremblay though the extent of the sentence is not listed as court records are not released to foreign nationals.

Our group purposefully selected this story as it was felt that the stories that are frequently seen on Facebook, of both Irish Nationals, and foreign nationals, being 'trapped' while attempting to groom what they believe to be young online user, might hit a little too close to home. But also, because we wanted to highlight to parents that it is not just malicious online users from Ireland they need to be concerned about. Some of these disturbed individuals are willing to travel thousands of miles to pursue the grooming of a child victim. Constant vigilance, monitoring and a proper understanding of the best safety practices where online security is concerned, should always be employed. We once again reiterate that we felt we could not ignore this area of research due to the risks faced by children online. It is certainly not the purpose of this report to scare parents, but parents must also recognise the danger is very real.

8.7 Risks of Unfiltered Access to Snapchat

The minimum age for Snapchat use according to their Terms of Services is 13 years of age and should be respected. Legally speaking if a child under the age of 13 is using snapchat with the consent of the parent, the parent assumes responsibility for any harm done. However due to a recent change to the digital age of consent in Ireland, this was amended from 13 to 16.

The Discover feature, as mentioned above, on Snapchat has very adult themes. An example would be a content creator called 'Brother' which discusses relationships and sex which are obviously very adulty themed. In one of their posts they feature a video of a girl undressing despite being filmed without nudity being show, in the eyes of an adult, it may be inappropriate for children. Examples are listed below which have been displayed on a test account create by our group where the age was set to 15 years old. To specifically test if these content creators were censored when using an account with its age set to under 18 the following still came up.

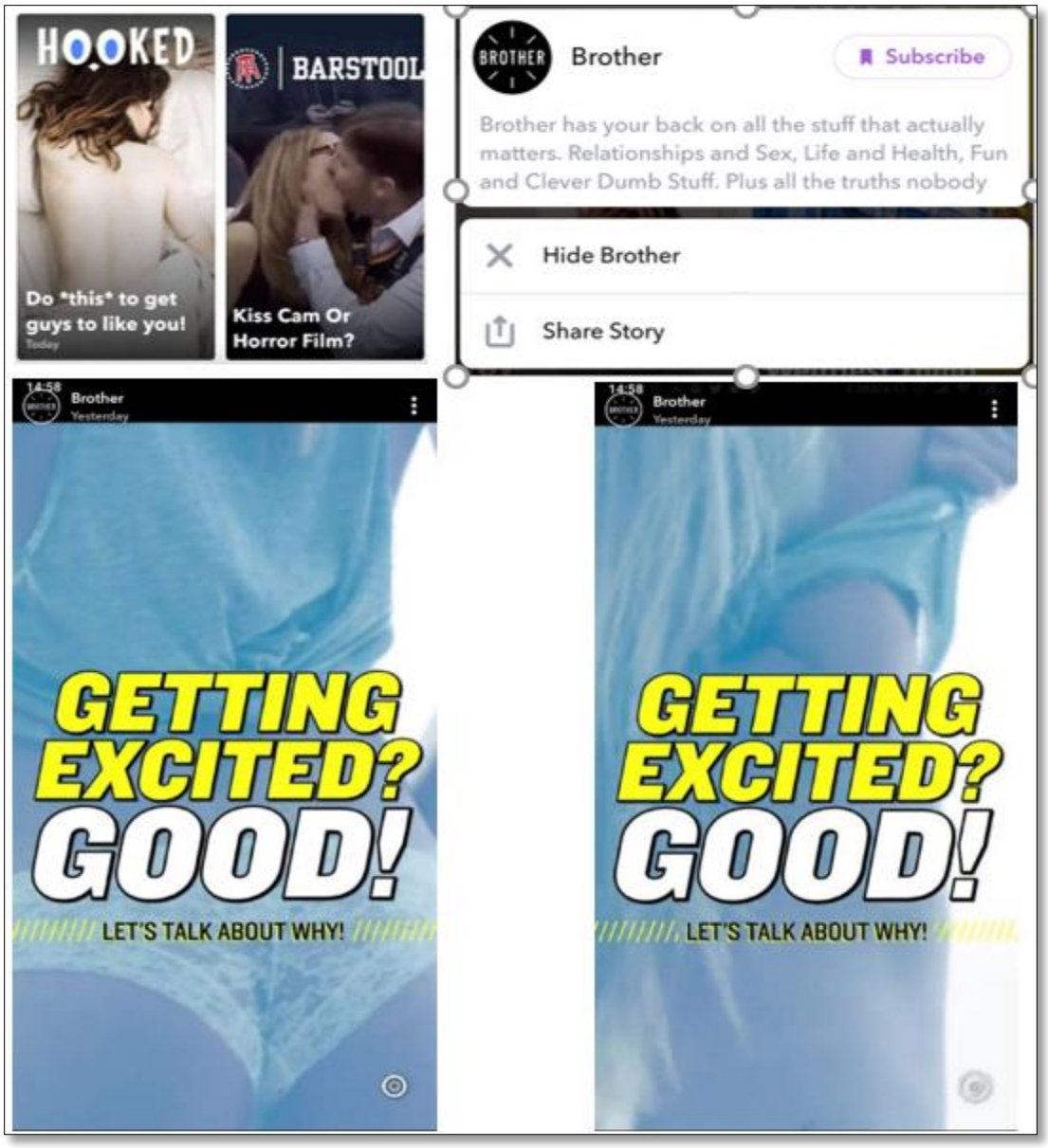


Figure 57 An example of inappropriate content for young children.

Snapchat unfortunately faces the same issues many other social media applications face; child predators on its platform. The police force in Humberside in the United Kingdom reported a total of 50 offences of sexual communication involving children between April 3rd, 2017 and January 3rd, 2018. Seven of these happened on Snapchat. In 956 cases of child grooming through social media, 20.1% of them was on snapchat. **(Miller C. 2018)**

Usually a snap will be deleted after a set period leading user to a false sense of security that the snap will be deleted. Children think this and often send silly or inappropriate pictures thinking they will be deleted. What some users don't know is that despite their snap being deleted from snapchat, a recipient can screenshot or record what they sent and keep it that way.

As previously mentioned, Snapchat's SnapMap feature allows users to track other users position in real time. This feature to track users is perhaps a very scary thought, particularly for parents. Combine this with the knowledge that predators are using Apps to groom children may lead to the question as to whether Snapchat's age restriction should be raised, or children banned from it entirely. However, there may be another, less restrictive, way of keeping children safer. Parental guidance of children about safety practices coupled with the proper modification of in App settings would increase App Safety. We hope our platform will help with this and we will cover guidelines to reduce the online footprint of Snapchat users in a later section.

There are also "Hacked" versions of snapchat which give those who use it special features like Geographic spoofing which fakes your location on the SnapMap, disabling the screenshot log which tells users who screenshots their snaps and other features. Snapchat states clearly in their terms of service that the use of these Apps is not permitted and whoever is caught using them will be banned. Despite this, it does not prevent predators from using it. **(unlimapps.com 2016)**

The Our Story feature on Snapchat is also potentially dangerous as children can add to the map their story and anyone can see it without being on their friends list. Then a predator could move to that location and add a snap to Our Story to start a dialogue between them.

8.8 Risks of Unfiltered Access to Instagram

As indicated by a graph from Statistica.com there are currently one Billion monthly active users on Instagram as of June 2018 **(Statistica.com 2019)** Out of those numbers, the main user groups are 18-24 and 35-44.

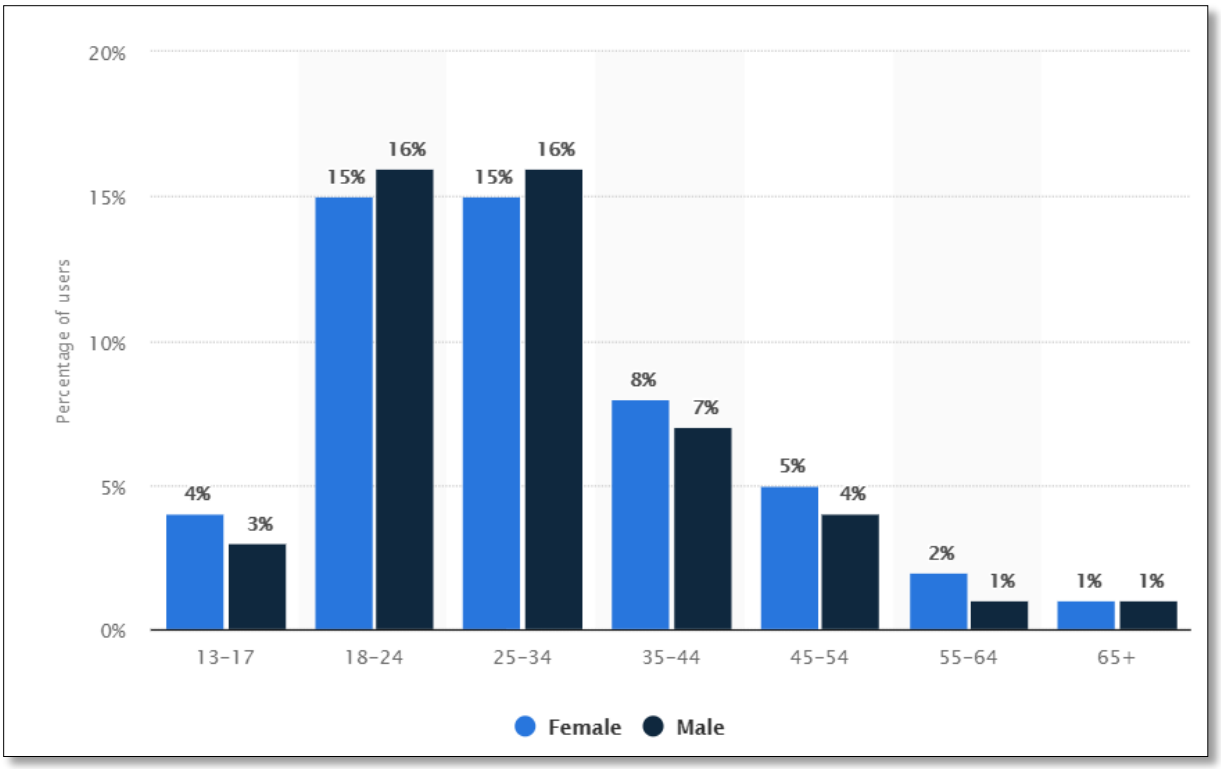


Figure 58 Statistics on percentage of active users on Instagram, split by age range and gender ***(Statistica.com 2018) [Accessed Feb 2019].***

It also shows that 7% of the active userbase are in the 13-17 range, meaning approximately 70 million are within this age range. It is also reported that 52% of teens use Instagram.

Business are using the platform to promote their brands through posting pictures and videos of their content. With these there are 2 million advertisers, up from 1 million back in March 2017 per month**,** with mobile advertising revenue of approximately 7 million dollars. **(Ahlgren M. 2019) (Lou C. 2016)**

There is also a large amount of celebrities that use Instagram to promote their 'Brands' and to engage with their fans. Many celebrities often use the platform to promote their own brand, however many are also paid by companies to promote a brand to their fanbase, it is often not clear that they are being paid or just like the product.

Figure 59 A sponsored photo from Kylie Jenner's Instagram page ***(Jenner k. 2018) [Accessed March 2019].***

As seen above, we have a celebrity advertising a product on her personal page, and the only way to tell it is a paid advertisement is via the hash tag #ad displaying in the inline txt with in the pictures tag.

8.8.1 Data Breaches

As noted in this article **(Techerati 2017)** The last data breach on Instagram took place in September of 2017, in which six million users had their phone numbers and emails exposed, these details ended up being sold on a searchable database known as 'Doxagram', selling for $10 a search. The database has since gone offline but is most likely in the possession of the hackers, and likely available on the dark web, this was confirmed by CEO of Instagram on the official Instagram Tumblr, however the exact numbers is not mentioned in this article **(Krieger M. 2017)**.

There was another data breach that took place in December 2018, however it was a Facebook data breach and would only affect accounts that use the Facebook Log in feature. **(Rosen G. 2018)**.

8.8.2 Instagram Inappropriate Content

On Instagram there is a noticeable amount of inappropriate content found on the platform. Firstly, inappropriate content can be found on the Instagram TV (IGTV) feature in which, by accessing via an account were the age is set under 18 years old (15 years old to be specific) the first clip found was a woman stripping and changing on camera. This could be inappropriate for children of this age.

Below is an example of a very quick search, which lead us to an account containing pornographic material of a very explicit nature. Finding this material was as simple as searching the word “hot” in the search feature.

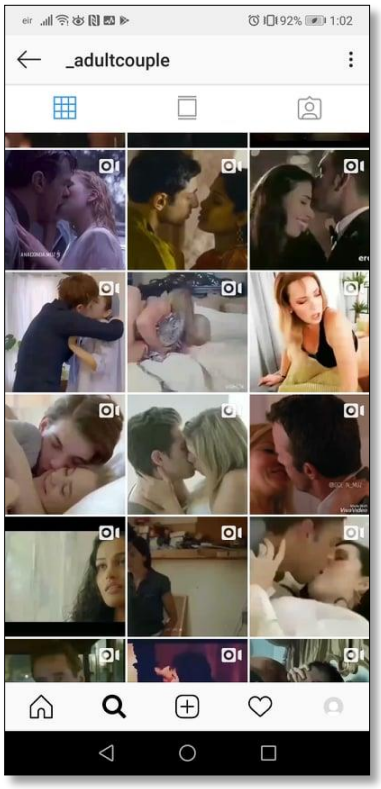


Figure 60 An example of potentially age-inappropriate material from Instagram ***(AdultCouple 2019) [Accessed on 20th March 2019].***

There is also a known phenomenon of Instagram models, that post suggestive photos on the platform, to garner likes and attention, they use this attention to try sell naked photos to individuals. These are easily accessible from anyone that has access to the platform. As you can see in figure 61, there is an account with next to nude models in all their pictures with links to a porn website.

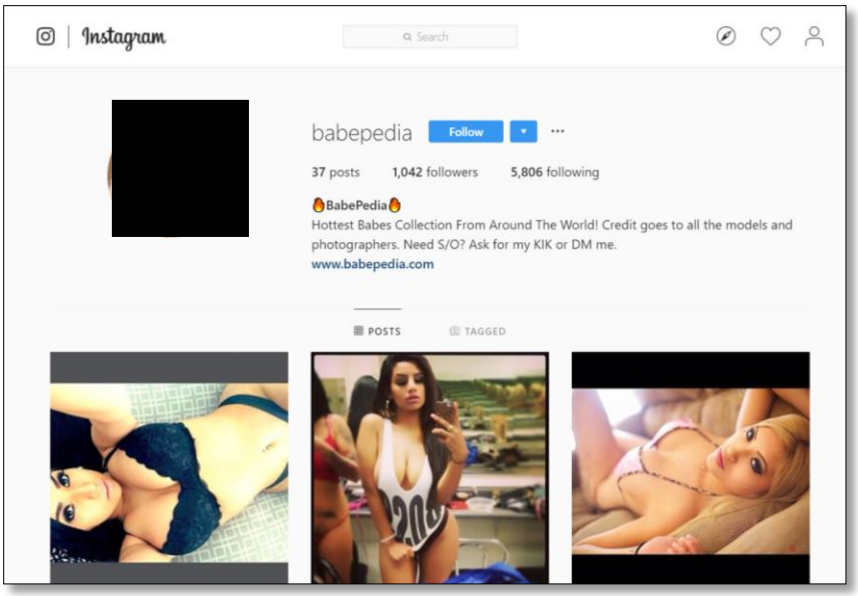


Figure 61 Babepedia Instagram profile with a link to their pornagraphic website.

There has also been a rise in fake celebrity accounts that are often used to groom children. They pose as these celebrities to try get in contact with underage users. To combat this, Instagram has a verification service, which enables celebrities to prove that the account is their own. Verified users will have a blue tick beside their name. If it doesn't have a tick, it's is likely a fake account **(Instagram 2019)**.

Figure 62 An example of three fake celebrity accounts, one being a parody account ***(Computer Hope 2018) [Accessed Feb 2019].***

8.9 Risks of Unfiltered Access to WhatsApp

At the time of researching this document, one of the biggest scandals is the internet phenomenon known as Momo, or the Momo Challenge. For context, the Momo challenge, is alleged to be an App based text challenge designed to elicit information from the user, and which also allegedly encourages users to self-harm, the Momo challenge is alleged to be a viral game that is said to be shared on messaging services like WhatsApp.

The premise of Momo is that when a child messages Momo, they are allegedly sent creepy messages and are ordered to perform violent acts, these acts escalate into even more extreme acts, until the child is ordered to commit suicide **(Sakuma A. 2019).**

There have been stories claiming that the terrifying images of Momo has been appearing on videos of Peppa Pig (a well-known children's animated show) and gameplay footage of Fortnite (a popular video game amongst children) posted on YouTube, and as stated on the Vox report mentioned above, it is now said that the challenge has spread to Snapchat.

However, a thorough search of YouTube reveals no evidence of these videos existing. Google, being the parent company of YouTube. has also released an official response on their own support website about the Momo challenge in which they stated they have had no evidence of any videos promoting the Momo challenge, and that such videos are against their policies, and that they encourage any incidences of the Momo challenge to be reported to them immediately. Videos that do discuss, report or educate about Momo on their platform are still permitted, and with it, images of Momo are allowed within the thumbnails of videos however the image is not allowed to appear on YouTube Kids **(Julia, Google Employee 2019)**. To confirm this, we tried to find Momo on the YouTube Kids App, however our attempts were unsuccessful.

The challenge is linked to is a statue called "Mother Bird", which was created by Japanese artist Keisuka Aisawa, the sculpture originally had nothing to do with the challenge, and in fact predates the challenge by two years, upon learning that the sculptures image was being used for such intents, he promptly destroyed the Mother Bird sculpture, stating in an article by The Sun, that he felt "responsible" for terrifying children with his work, but also emphasising that 'Momo is dead, she doesn't exist and the curse is gone' **(Reilly J. 2019)**.

What lead to the growth of the Momo challenge was that it was suspected to be connected to the suicide of a 12 year old girl in Argentina in august 2018 **(Kelleher P. 2019)**, however after several days of researching, we were unable to find any reputable evidence available online, this did not stop the media hype from escalating and spreading globally at a tremendously fast rate, Despite the fact that no documentable evidence that supports the alleged offending material.

Following on from the alleged tragic Argentinian suicide, the challenge is said to have spread further to Mexico, with an official newsletter published by the Office of the General Prosecutor of the State of Tabasco, warning citizens about "El Momo" **(Office of the General Prosecutor of The State of Tabasco 2019)**.

This highlights a worrying trend, with the story appearing to be spreading rapidly, despite no evidence being presented of the existence of the alleged offending material., This however does not prevent official sources from presenting warnings, which treats the allegations as fact.

The fear surrounding Momo made its way to the United Kingdom and Republic of Ireland in the beginning of 2019, with schools, police services and Governments globally issuing stern warning to parents, A prime example being the Police Service Northern Ireland issuing a warning about the "Dangers of Momo" **(PSNI 2019).** However, as stated above, these warnings are unfounded and are based on hearsay.

The story was elevated by tweets warning about the scandal, even famous Instagram star Kim Kardashian posting about the subject on her Instagram story.

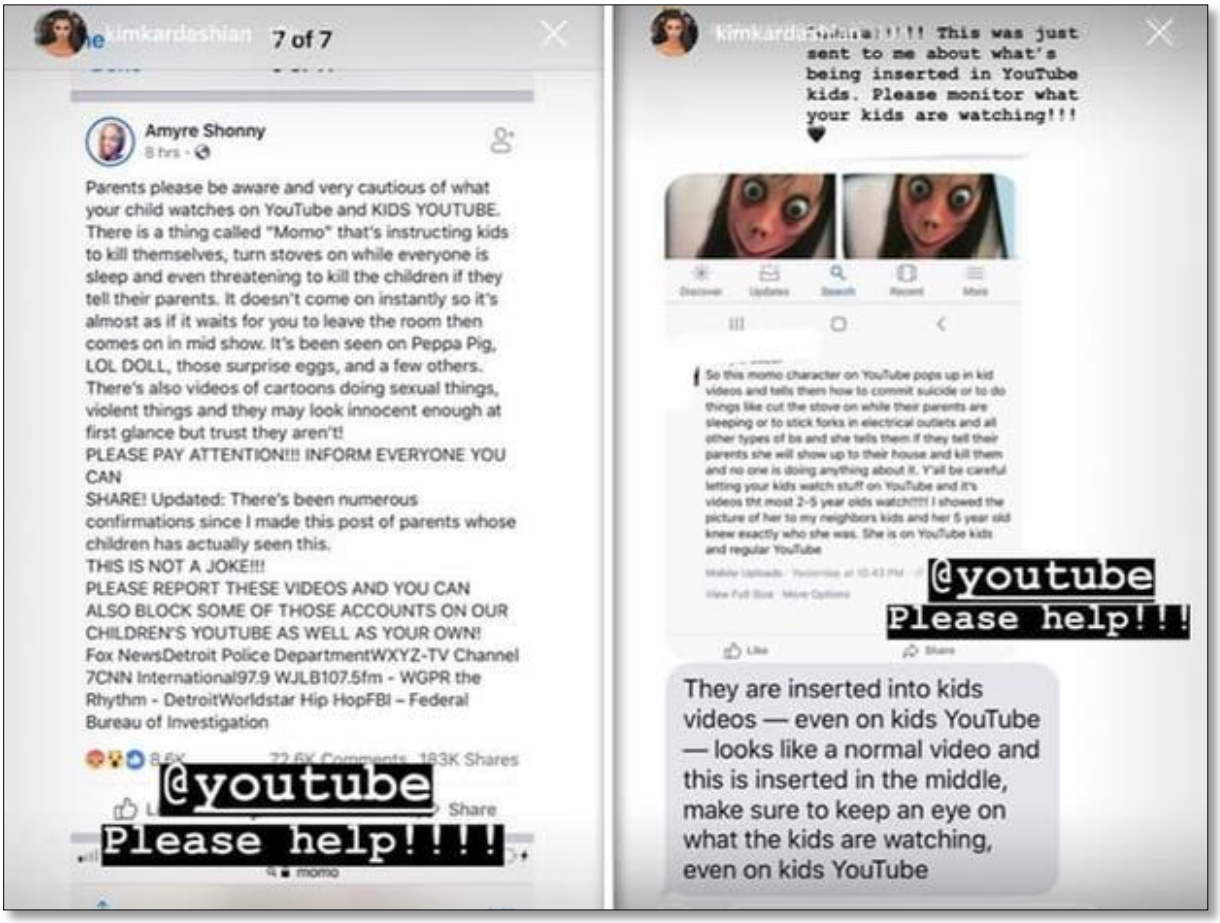


Figure 63 Kim Kardashians Instagram post about Momo ***(Lewis S. 2019) [Accessed Feb 2019].***

This only succeeding in adding more unjustified hysteria into the minds of parents. It wasn't until organisations like The UK Safer Internet Centre, CyberSafeIreland and many children's charities began denouncing the Momo challenge, calling it "Fake News" **(Curley C. 2019) (Waterson J. 2019)** that the hysteria began to fade. Many of these organisations stated that in fact these news outlets were causing more harm than good, due to the large amount of false data being spread around, causing the hoax to grow on its own. After this, many news outlets began to publish articles about how the Momo challenge was a hoax based of legitimate research.

Through researching of this paper, it is very obvious that a lot of the hype of this phenomenon was due the vast number of parents who do not have an understanding on how to protect their children on the internet. All of this culminated in the Momo Phenomenon becoming larger than it originally was and highlighted a necessity for parents and children to be educated more on Internet safety, and how to implement security features on a device that is used for a child. But most importantly it highlights how parents must try to leave an open dialogue between themselves and their child when it comes to Internet safety, so that if there was a dangerous situation taking place online, be it hoax or not, then the child would feel safe in confiding with a parent.

8.10 YouTube / Google Family-Link / YouTube Kids Case Study

The most obvious dangers of exposing children to unfiltered YouTube content would be allowing them to engage with strangers online through the comments section where anyone can inspect your profile and gather information about the user and see videos they have publicly uploaded.

However another issue that is likely less known to parents refers to an incident known as "Elsa-gate" **(Subedar A. and Yates W. 2017).** Elsa-gate is a controversy to do with videos suggested by YouTube for kids and even on the YouTube Kids App which contain themes that are extremely disturbing and inappropriate for children. The videos could contain things such as violence, sexual situations, drugs and alcohol and much darker situations. The videos may contain popular Disney characters or people dressed up as them part taking in these acts.

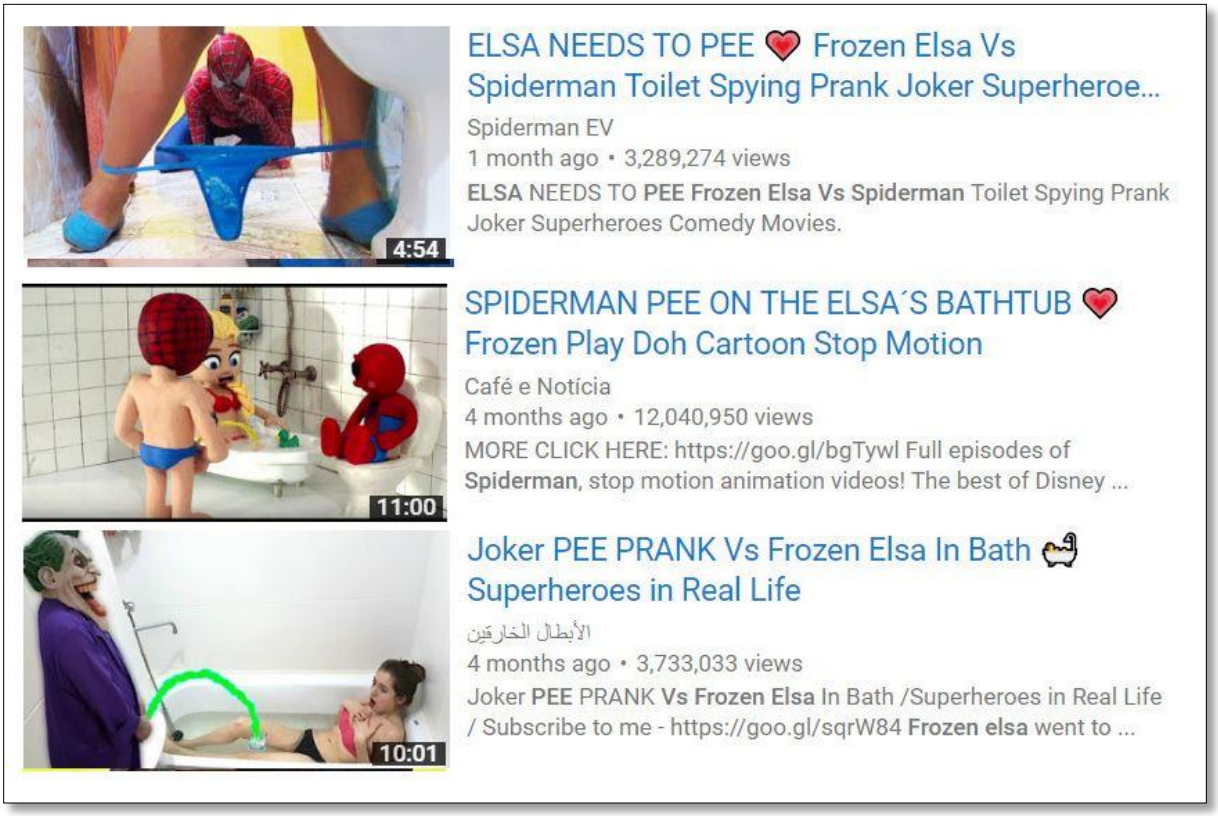


Figure 64 Here we see an example of some videos that fall into the Elsa-gate category of videos.

The reason these videos were suggested as suitable for children is because of the tags the uploaders used when adding the content such as "education" and give them titles with Disney characters in the title. Even though this abuse of the terms & conditions, the YouTube algorithm thinks these videos are made for children and sometimes these videos slip through the cracks in YouTubes Child Safety Algorithm. Above, is a screenshot taken from YouTube of these inappropriate videos **(theouterlight 2017)**. You can also see just how much views these videos are getting, ranging from 3 million to 12 million views.

As of researching this document a new scandal has come to light. This scandal does not pertain inappropriate videos but comments on innocent videos. This scandal highlights the danger of children uploading their own videos on the YouTube platform. On the 17th of February 2019, the YouTube Channel "MattsWhatItIs" posted a video entitled "YouTube is Facilitating the Sexual Exploitation of Children, and it's Being Monetized (2019)" **(Watson M. 2019)**. Matt Watson, the owner of this YouTube channel, talks about how YouTube is being abused and made to be a source for child abuse. He goes on to talk about how children are innocently uploading videos doing gymnastics or showing off their new clothes they bought. Although the videos are uploaded innocently enough, in the comments are found suspicious timestamps. A timestamp on a video allows commenters to reference a specific time in the video and allows users to click on the timestamp and view the video at that specific time. In Matt's video he goes on to talk about how paedophiles are using timestamps to select specific times in the video where children are in exposing positions that may display partial nudity.

In his video he goes on to show that not only are paedophiles abusing the comment section to share moments in kids' videos where they are in exposing positions , but that if you click on a few of these videos in succession then you will be recommended more of the same video that contains children in exposing positions allowing paedophiles to browse these videos easily and search for more.

The reason YouTube is recommending these videos is because of the recommendation algorithm **(Trouvus 2019)** which recommends users videos based on their watch history. YouTube have since responded and adjusted their algorithms to reduce this recent abuse. **(YouTube, 2017)**.

This shows us that there is very unsuitable content for children on YouTube both creating content and viewing content and leads to the debate should children use it at all?

9.0 App Safety Rating System Breakdown

Our App safety rating system is based on a simple points system that awards points where safety systems have been set in place that specifically serve to reduce visibility and the user's online footprint. Please note, the scoring system of our guide is based on our best practice recommendations (to be presented later in this document) being fully implemented. The scoring system is as follows:

1. Encryption:
Yes = 1 No = 0.

Is the data in the App encrypted?

2. Does the App have an Invisible mode:
Yes = 1 No = 0.

Or The ability to significantly reduce online visibility.

3. Data Shared to Third Parties:
Yes = 0 No = 1

This includes marketing agencies or companies who run data centres outside the main organisation.

4. Does the App contain GPS tracking:
Yes = 0 No = 1

5. If so, Can the tracking be turned off:
Yes = 1 No = 0

6. Does the APP contain the ability to remotely delete data from contacts, chats, groups etc?
Yes = 1 No = 0

7. Can users be searched:
Yes = 0 No = 1

Especially worrying if the users are not connected

8. Does the APP contain any parental controls:
Yes = 1 No = 0

9. Does the APP contain the ability to directly report/block users:
Yes = 1 No = 0

10. Is the APP GDPR compliant and possess the ability to request user data to examine what data is being collect and/or shared:
Yes = 1 No = 0.

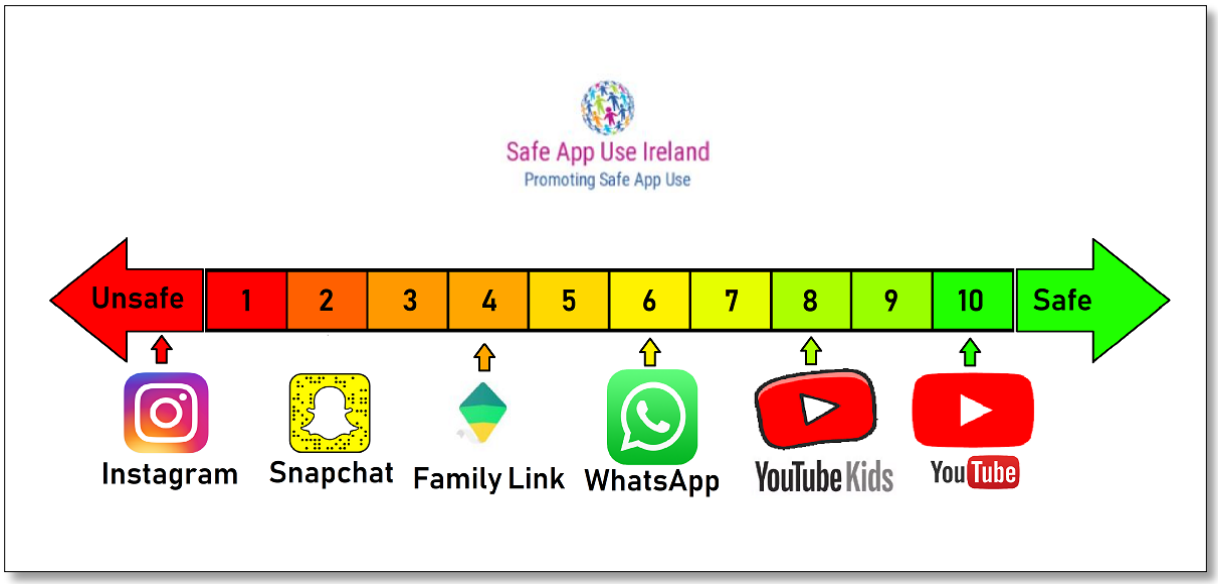


Figure 65 Our App Rating Graphic

10.0 Brief explanation of VPN's

VPNs are a relatively new addition to online security but the use of them has exploded in recent years. But what exactly is a VPN? Should you fear them? Should you use one?

A VPN, or virtual private network, is a service which serves to hide a user's IP Address. Essentially, the user connects to a server provided by the service provider host. This server assigns a new public IP address to the user. Each time the user requests information via the internet they request it through the VPN server, which forwards on the requests as though it where the server making the request, using the users assigned public IP address which was issued by the VPN server. When the requested information is returned to the server, it is forwarded to the users actual public IP address which only the VPN server can see. Some services can detect that the user is using a VPN, but they cannot detect the actual real public IP address of the user.

Many have, in the early days, feared the use of a VPN, perhaps due to a stigma related to the use of VPN's by 'hackers' mistakenly believing this will perhaps paint them in a negative light or draw attention to them.

Should you fear a VPN, or the use of a VPN? Absolutely not. VPN's are very user friendly and provide an extra layer of security.

Should you use a VPN? While it is not strictly necessary in day to day life to use a VPN, we do strongly recommend the use of a VPN. Currently our top recommendation for a VPN would be ProtonVPN.

What can a VPN provide in terms of security? Well, while we shall refrain from getting too technical, a VPN allows a user to obfuscate their actual location. As you will see in a demonstration in our research outcomes, a user can be in one city in Ireland, but be displayed in App as being in a totally different country. This could potentially cause issues with tracking your child or their device if you are a concerned parent, so it is important to teach your child the basic use of a VPN and to have it deactivated should you wish to find them or their device.

Where firewall rules in an unfamiliar internet access zone are preventing you from accessing trusted services, VPN's can sometimes allow a user to bypass these restrictions. This is a double-edged sword however, and if there is content you do not wish your child to access which you have blocked via your router or internet firewall, a VPN might allow them to bypass these restrictions.

We feel that while there are potentially a few drawbacks connected with VPN use, our group feels the benefits out weight the risks. The ability to hide your child's location, preventing potentially dangerous Apps from leaking their location to potential malicious users or predators alone merits the use of a VPN.

11.0 Primary Research Outcomes

11.1 Snapchat

Snapchat is a social media platform that has spread like wildfire among the children in Ireland with 84% of 15 to 18-year olds owning an account and 85% of them use it daily **(Heneghan C. 2016)**. Snapchat allows you to use pictures or "Snaps" (See Appendix 1) to talk with friends, sometimes pictures contain a message and sometimes it doesn't. Users can also share a snap or video to another user allowing them to see what they want. Users can also build streaks which are consecutive days in which two users have sent snaps to each other. The streak is displayed beside the user's name and is viewed as a symbol of friendship as it takes requires each user to send each other a snap each day to each other.

11.1.1 Snapchat Terms & Conditions:

Snapchat's Terms of Service **(Snapchat 2018)** were designed with the aim of making it as readable and easy to understand as possible. You cannot use Snapchat without accepting the Terms & Privacy Policy. Below is listed a distilled version of the terms and conditions mostly pertaining to safety regarding children that parents may want to know the aim is not to encourage parents to ignore the actual terms and conditions but to highlight the importance of what is often overlooked if they are ignored.

- No one under the age of 13 may use Snapchat.
- You must not be barred by law to use Snapchat under your country's jurisdiction.
- When creating content on snapchat (taking pictures, posting them online) you retain the ownership rights of it. However, you grant Snapchat and their affiliates the right to use that content royalty-free however they please if you use the Services.
- You allow snapchat to use the data they collect on you to perform targeted advertising based on this data.
- Snapchat does not review all content on its platform however reserves the right to review it and remove any content that may violate the Terms and Conditions, Community Guidelines or the Law.

The following bullet points are under snapchats safety terms of service.

- No one may use the services for anything illegal
- No one may use any automated means to interface with the services.
- No one may create third party software that interacts with the services or the data of the users who use it.
- No one may use the service in such a way that would damage the performance of the service or inhibit it completely.

- You will not attempt to login to another users account without consent.
- You will not attempt to gain the login credentials of another user without consent.
- The posting of incitements to violence, hate speech, threats, graphic violence or pornography is strictly prohibited.
- You will not upload viruses or other malicious code or otherwise compromise the security of the Services.
- You will not attempt to bypass content-filtering techniques Snapchat uses or try to access features or areas of the Service that you are not allowed to use.
- The Scanning, probing or testing the vulnerability of any of the services or any system or network is strictly prohibited.
- The encouragement of breaking these terms of service is strictly prohibited.

Snapchat collects information from its users when they use the services. They collect the following but is not limited to:

- How you use Snapchat:
  How you talk to other users, when you talk to them, which friends you exchange messages with the most and how much you talk to them.
- What you make on snapchat:
  What you make on snapchat such as stickers and the meta data associated with them**.**
- Device Information:
  What information your phone has stored on it including time zone, keyboard language, and what type of device you use like operating system and version.
- Device Phonebook:
  There is an option to allow Snapchat to view your phonebook on your device.
- Camera roll on your Device
  Snapchat has access to the photos saved to your device.
- Location Information:
  Using a multitude of techniques, Snapchat gathers information on your location based on region settings, WI-FI access points and other techniques.
- Information Collected by Cookies and Other Technologies:
  Snapchat uses cookies and other technologies to gather information using unique advertising identifiers.

- Website Information:
  Snapchat collects information on you when you use their website online. They collect data such as your IP Address, what you did on the website, pages viewed and similar.

- Information Collected from Third Parties
  Snapchat collects information on Third Party Apps you may have used that ties into Snapchat like Bitmoji.

Below is an excerpt from Snapchats Terms and conditions specifically talking about information that may be collected from users under the age of 13.

> "Our services are not intended for—and we don't direct them to—anyone under 13. And that's why we do not knowingly collect personal information from anyone under 13. In addition, we may limit how we collect, use, and store some of the information of EU users between 13 and 16. In some cases, this means we will be unable to provide certain functionality to these users. If we need to rely on consent as a legal basis for processing your information and your country requires consent from a parent, we may require your parent's consent before we collect and use that information." **(Snapchat 2018)**

All the information gathered above can be viewed in full on snapchats website under their privacy policy. **(Snapchat 2018).**

Community Guidelines:
The Community Guidelines are as follows and can be found on snapchats website under community guidelines **(Snapchat 2018).**

Sexually Explicit Content:

- Promoting or distributing pornography is strictly prohibited.

- Non-sexual contexts of nudity are not considered, for example breastfeeding.

- Sexual content of anyone under the age of 18, even of the user themselves may not be posted, saved or sent to anyone. You may not ask a minor to send explicit imagery or chats and the sexual exploitation of children is reported to authorities.

Harassment & Bullying:

- Bullying on the services is strictly prohibited.

- If someone blocks you do not attempt to contact them from another account.

- Do not take snaps of someone in private locations such as bathrooms, medical facilities or otherwise without consent.

Threats, Violence & Harm:

- Never threaten to harm anyone or anyone's property.

- Don't post snaps of graphic violence or animal abuse.

- The promotion of self-harm or eating disorders are strictly prohibited.

Impersonation & Spam:

- Do not impersonate other people or attempt to deceive others about who you are.

- Deceptive practices, spam and activities such as these are prohibited.

Hate Speech & False Information:

- Do not post content that promotes discrimination or violence based on disability, gender identity, sexual orientation, religion, national origin, ethnicity or race.

- The promotion of false claims or denying of tragic events is strictly prohibited.

Illegal Content:

- Do not use snapchat for any illegal activities.

Terrorism:

- Terrorist Organisations are strictly prohibited from using snapchat.

11.1.2 Snapchat Features

A "Snap" is a picture a person can take and put a message on top of it. The message and Snap are put together and sent privately to whomever the user chooses. The message is then deleted after a selected amount of time by the user. It can be set between 1 and 10 seconds or no timer can be set at all however the snap will be deleted once the user taps off the image. It is possible to save and share these snaps and send them to other people. Any snap you take can also be saved and become part of what Snapchat calls "Memories" which is a gallery of your saved media. It is also important to note that users can screenshot Snaps and save them to their device so the deletion period is not always final. There is also a chat function which allows users to engage in text-based chat, video chat or a voice chat. It's important to note that the text-based chat is default set to delete messages once they have been read unless a user highlights the text by tapping on it and saves it to memory.

Snapchat implements encryption on their service; however, they have a hardcoded encryption key to be able to access this information at any time. Attacks against this encryption have already been reported and documented by Gibson Security as discussed in by Czarina Lao, (et al) in chapter 4.1 of the paper **(Czarina Lao, et al, 2017)**. Gibson Security went on to release a full discloser about this security flaw. Naturally, this kind of encryption is very unsafe and led to approximately 4.6 million usernames and phone numbers being leaked. This hardcoded encryption might also potentially be used to access encryption information via main in the middle style attacks.

Another key feature of Snapchat is My Story. My Story is a chronological gallery of snaps you've uploaded to it in the past 24 hours **(Snapchat, 2015)**. When you add snaps to My Story, it can be seen by everyone on your friends list. The chronological aspect to stories makes them easy to understand unlike a news feed where new content is displayed first. On snapchat your story goes from oldest to newest so if you put a birthday party on your story, you could see the party unravel from start to finish which is usually how we tell stories to each other. People are also able to save each snap from a story, so the 24-hour deletion timer is not necessarily final. These stories can also be saved into your "Memories" and viewed later. Snapchat also has a feature called discover. Discover delivers content from publishers, shows and content creators.

The last three features of snapchat work in conjunction together. The Snap Map, Bitmoji and Our Story. The Snap Map is a map of the world which shows the live location of anyone who is your friend on Snapchat and has allowed Snapchat to track their position. It also shows what you are most likely doing based on your position (If you are in a shopping centre then you it shows you shopping and if you're listening to music then your avatar is too). Bitmoji is a third-party App that allows you to design your own 2d character to represent yourself. This avatar then shows up as you on your account. A user can also take a picture of themselves and have this as their profile picture.

Our story works together with the SnapMap. Unlike My Story, Our Story allows a user to upload any Snaps they want, to a gallery that can be viewed by anyone who has the App installed.
Our story works as a collaborative Gallery, meaning anyone who is nearby can add to it. Whenever someone uploads a Snap to Our Story a heatmap is generated on the Snap Map to show how many snaps people are posting in that area.

Figure 66 Picture of the SnapMap Feature of Snapchat.

11.1.3 Snapchats Personal Security Optimization Options

Snapchat allows the users to:

- Manage Who can contact you
- Manage who can view your story
- Manage who can see your location
- Manage who can add you as a friend
- Manage if you can be seen on Quick Add
- Manage Conversations (Delete messages)
- Manage Friends (Unfriend, Block, Report)

In the next section we will show how these actions can be done.

11.1.4 Snapchat Settings

Snapchat can be a very scary place for children to be. Despite this if the Apps safety features are used properly the risks that come with the App can be reduced. This section will detail the steps in which a parent or user can secure their account to prevent unwanted contact from individuals in Snapchat and protect themselves in a potentially predatory environment.

To start adjusting settings, swipe to the left screen where your friends are listed. Click on the icon at the top left as shown in figure 67. A new screen will appear. Click on the cog at the top right of the screen as shown.

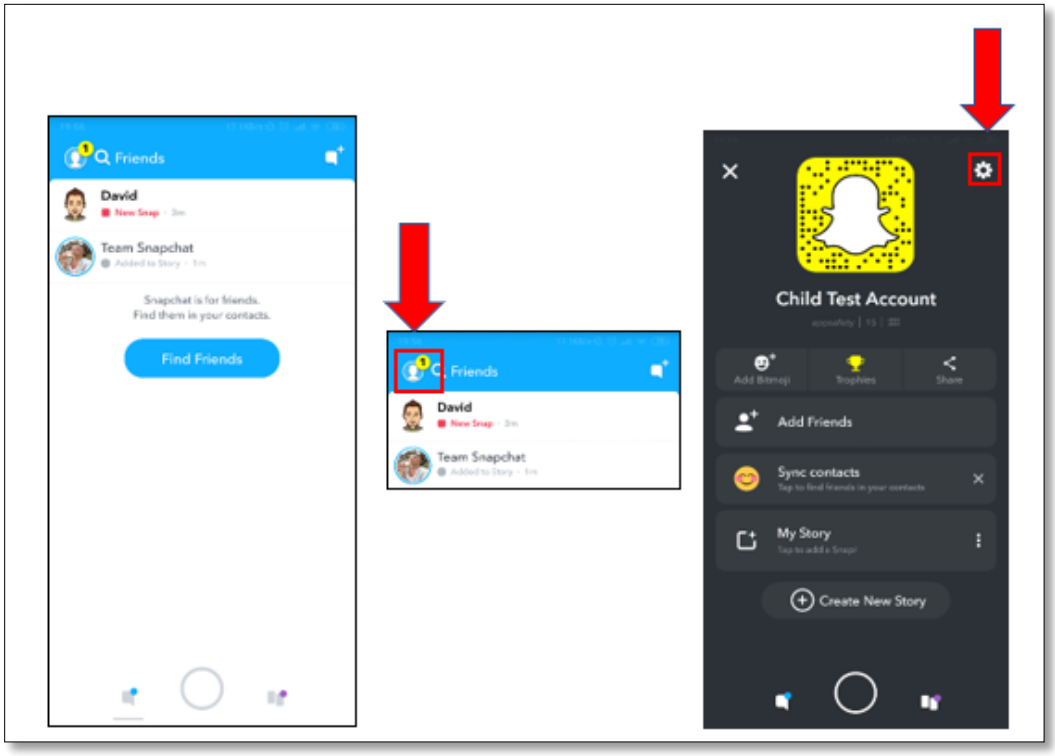


Figure 67 How to get to Snapchat Settings

Now the settings page should be open displaying your basic account information as shown on the left below in figure 68. Scroll down until you get to the "Who Can…" section as shown on the right below figure 68. Here you can manage 'Who Can' contact you, view your story, see your location and the option to disable being visible to add as a friend from mutual (friends of friends). To begin optimizing the account to create the safest environment, tap on "Contact Me".

Figure 68 Changing who can Contact you on Snapchat

The next screen will allow you to choose who can contact you directly with any communication, be it snaps, messages or calls. This setting should be set to My Friends only. This disables anyone whom you don't have on your friends list and only who you have accepted as a friend to contact you.

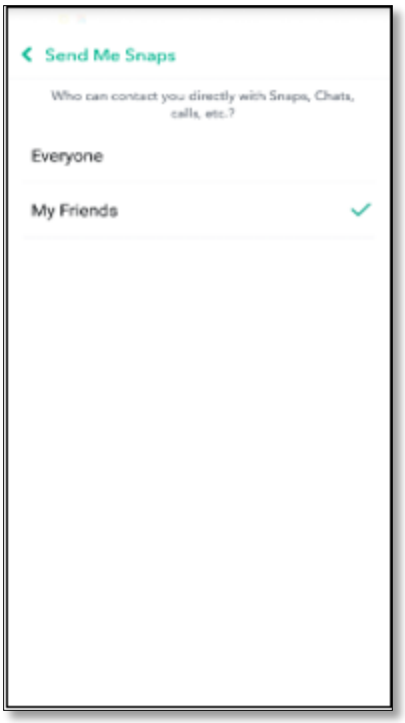


Figure 69 Above you can set who can send you Snaps.

The next settings we can optimize is the View my Story settings. Tap on “View My Story” as shown in figure 70. From here we can set who can view your story. It should be either set to “My Friends” or Custom. Custom allows you to specify exactly who on your friends list you don’t want to see your story which can be seen in figure 71.

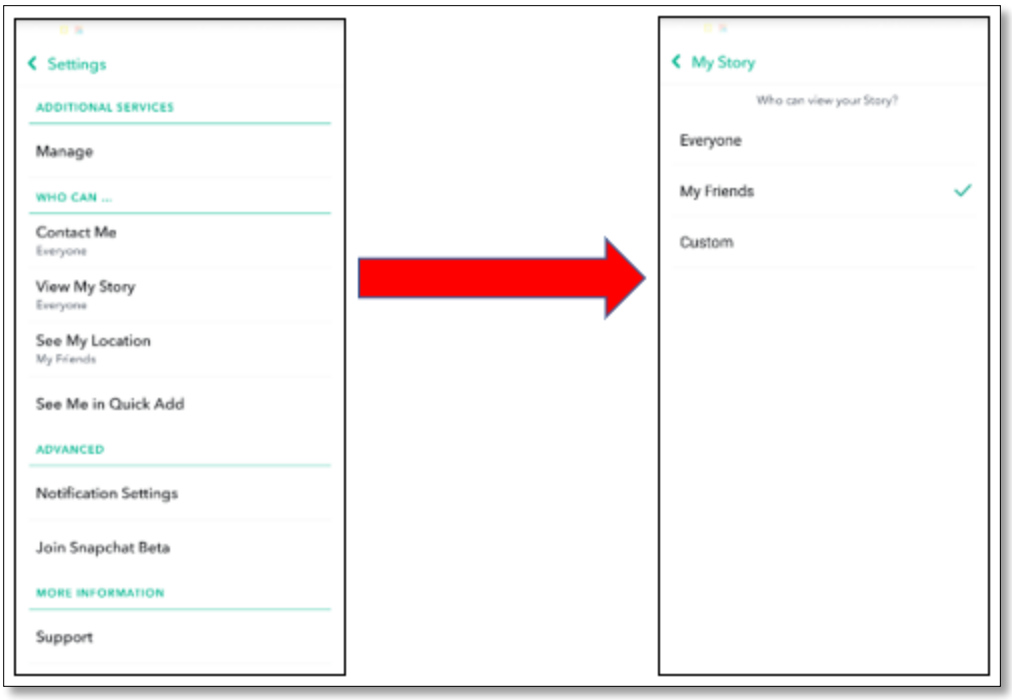


Figure 70 Accessing the Story settings.

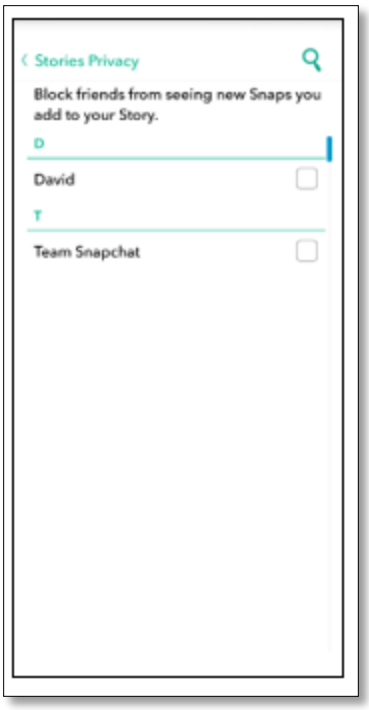


Figure 71 Control who can see your story.

Possibly the most important settings we can optimize is who can see your location. Select “See My Location” as shown in figure 72. Here you can manage who can view your location from everyone on your friends list or specific friends as show in figure 73. We recommend selecting ghost mode as shown on the right in figure 72 as this always hides your location from anyone and unticking the allow friends to request my location.

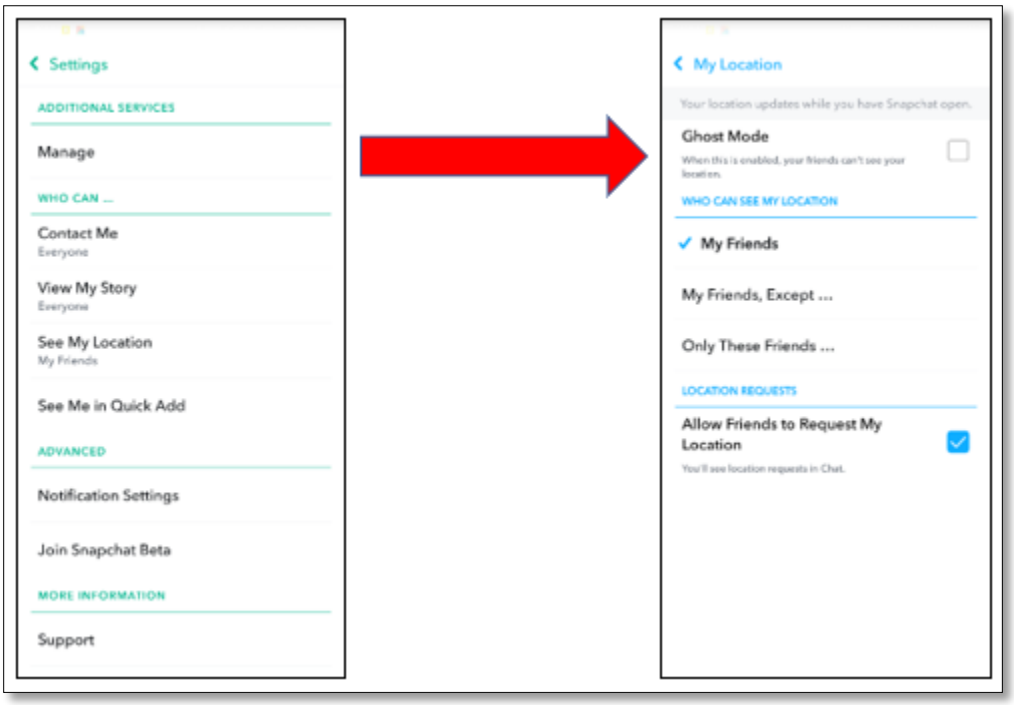


Figure 72 Managing Who can see your Location in Snapchat.

Figure 73 Selecting specific friends who can see your location in Snapchat.

The final setting required to be changed is “See Me in Quick Add”. Quick add allows users to add users to their friend list off another friend’s friend list. To stop your account from being shown on these lists, make sure “Show me in Quick add” is disabled as shown in figure 74.

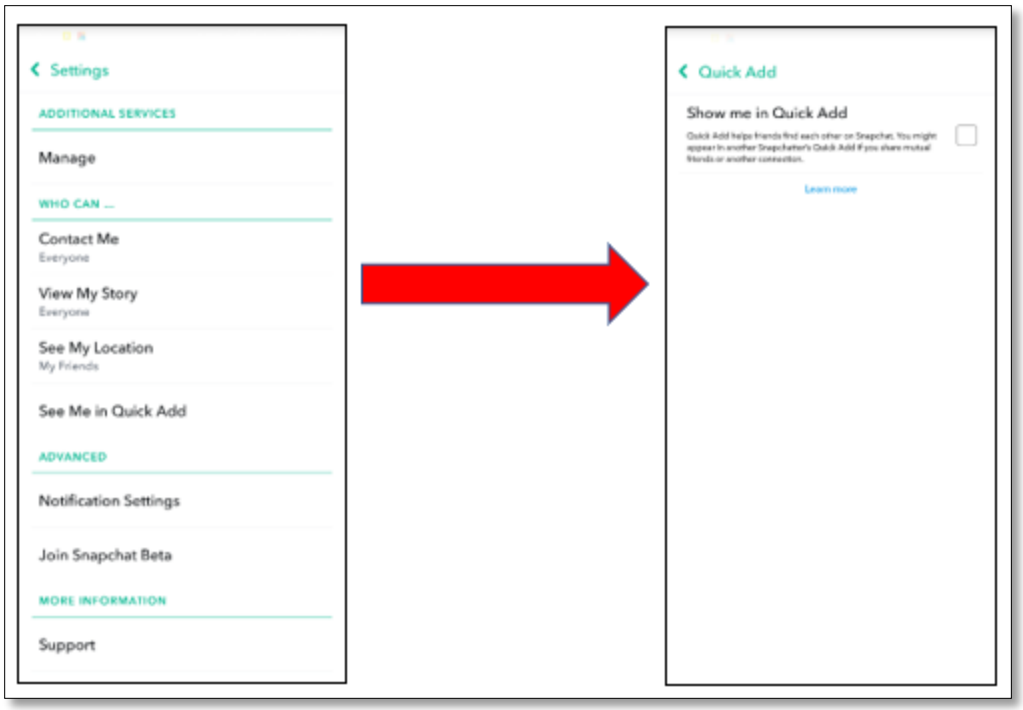


Figure 74 Managing the Quick Add Function in Snapchat

11.1.5 Blocking Users

To block a user, tap and hold on their name in the friends list (as shown in figure 75) and the settings for their user will appear. Tap on "Settings" and a new menu should pop up as shown below. Here you can manage the settings for this friend, options include Edit Name, Do Not Disturb, Mute Story, Clear Conversation, Remove Friend, Block Friend and Report as shown in Figure 76.

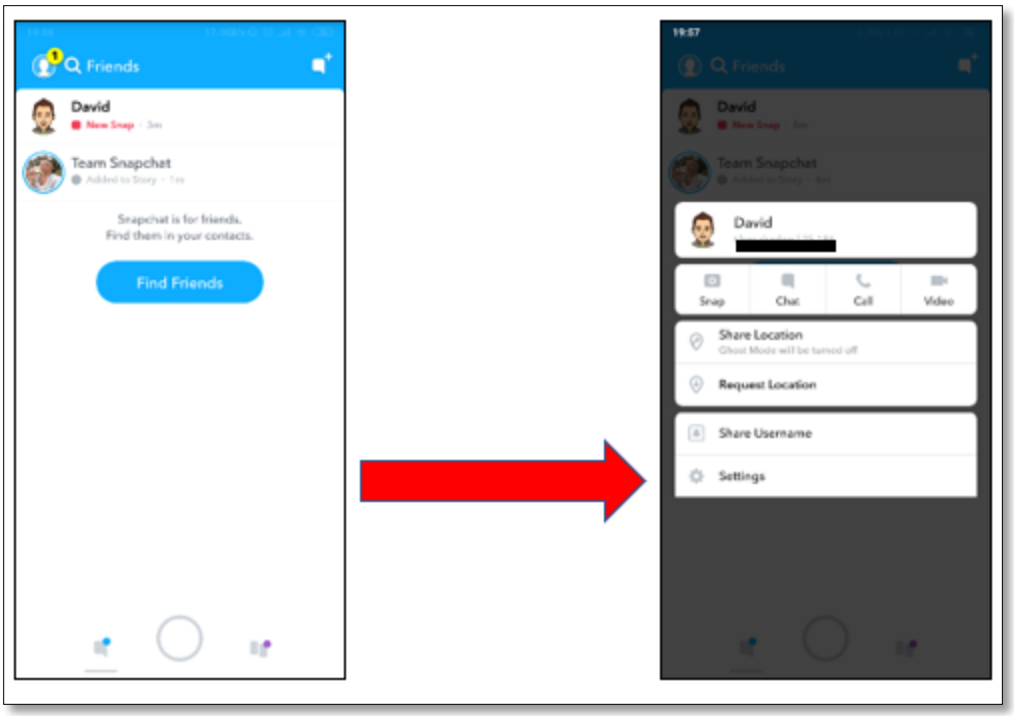


Figure 75 Managing Users in Snapchat

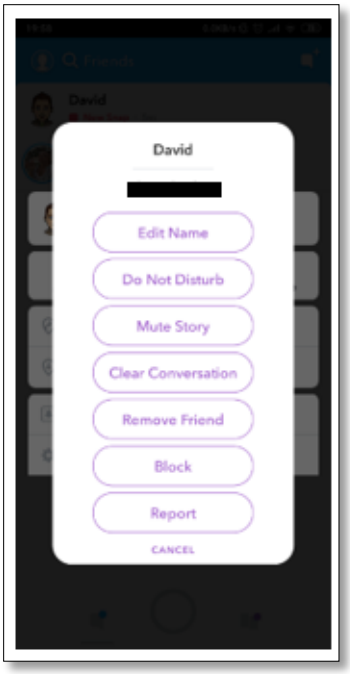


Figure 76 Managing Users in Snapchat

11.1.6 Snapchat Best Practice Settings Guide

Having reviewed the settings, we will now offer a best practice guide to the settings we suggest be employed to better protect the child's use of their Apps and their device to increase their safety while accessing online content via Apps:

- We Recommend to only allow friends to send snaps to the user preventing anyone who is not your friend from sending you messages
- We Recommend that only selected (Custom) friends can view your story
- We Recommend that ghost mode be turned on, so no one can see your Location or allow the use of Our Story.
- We also recommend unticking the allow friends to request my location option.
- We Recommend that you do not enable to be seen in Quick Add

11.1.7 Snapchat App Safety Rating

Based on our custom App safety rating system and our best practice guide being fully implemented the Snapchat App scores as follows.

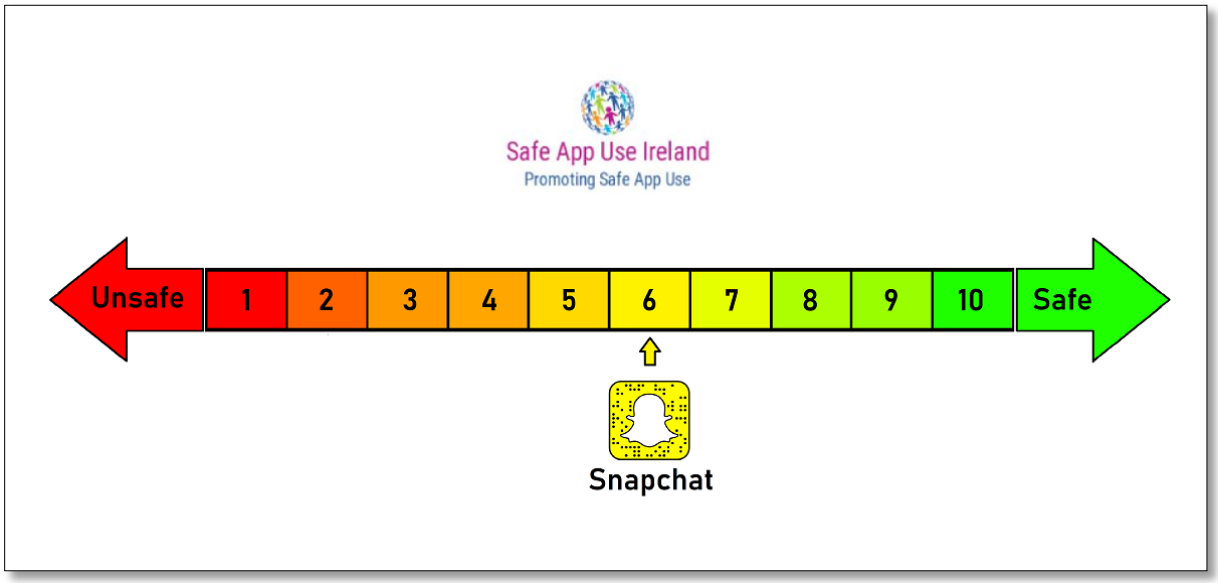


Figure 77 For Breakdown of Points System, please see: 10.0 App Safety Rating System.

11.1.8 Reflections on Snapchat

While Snapchat offers privacy and safety options for most of its features, some features are left without any consideration to these topics. The Our Story function for example which, by its very nature, allows anyone in the world to view content you specifically want the world to see. Obviously, this was a deliberate and honest feature created by the Snapchat team, however, it raises the question as to what the digital age of consent should be set to, or rather the age at which people should be using Snapchat at. The reason why this is concerning is because our story feature allows minors to broadcast their geolocation whether knowingly or unknowingly.

As is common place within major corporations, data is shared between partners and potentially third-party data storage locations. This increases the likelihood of data breaches. While this third-party sharing of data between partners is commonplace, this also comes with an inherent risk of user data leakage.

While all the features on Snapchat can be configured and set in a way that only allows certain users to see your story, talk to you and see you on the SnapMap, it must also be considered that a child in question may change the settings when a guardian is not around. Should Snapchat be used without implementing the highest levels of safety we consider it to be a very unsafe App, particularly to children. We do not feel that using Snapchat is suitable for minors, because of this we suggest that Snapchat must be used, if at all, within direct supervision and using the full extent of its safety options. Therefore, the score of six is only applied if the highest security settings are applied.

11.2 Instagram

Instagram is social media application available on all popular mobile devices, the application can be accessed through a computer, however most of its features, like sending messages, uploading content, etc. are only available through the mobile platform. It allows you to post photos and videos, add filters to said photos and videos and to view other people's uploads. The platform also allows you to follow other people, so you can see their content more easily, having their content presented to you as the first thing you see on your homepage, or "timeline".

There are several different types of content that can be posted on Instagram, from videos and photos that can be posted on the users own page, to the story photos that can be posted on a section accessible by clicking the users profile picture, or accessible from the timeline section by the users followers, these stories are only available for twenty four hours, however the stories can be added to a section available on the users page to be stored and accessible indefinitely.

11.2.1 Instagram Terms & Conditions

As with every product that must be signed up for, there is always a terms & conditions, or terms of service attached to the product, Instagram is no exception.

We conducted our research by exploring the terms & conditions of Instagram to find anything that might be of concern to parents when it came to their children access to the application. We then condensed this material into a more presentable format to make the information we felt most important to parent easier to access. The intent is to highlight the importance of investigation terms and conditions, not to facilitate the skipping over difficult to read material.

Who Can Use Instagram:

When it comes to Instagram, they want to have their platform as open and inclusive as possible, however they also want users to feel safe and secure, in accordance with the law. As a result, they have implemented a few restrictions to the platform:

- The minimum age to be on the platform is thirteen years old.
- If you had previously had an account which had been previously disabled for violation of the law or any of Instagram's policies, you will not be allowed to reactive that account.
- You must not be a convicted sex offender. This stance could be reassuring to parents where their child has a less likely chance to meet a certain individual. More importantly, if they should discover a registered offender, they can be assured that upon reporting the offender he or she will be removed from the platform.

How You Can't Use Instagram:

To provide a safe space for you and your kids on Instagram, they have provided several guidelines of things which you can't do on Instagram, as in to protect users of their community.

- It is against their guidelines to impersonate other individuals or to provide inaccurate information, although you don't have to publish your personal identity on Instagram, you still must provide Instagram with accurate and up to date information as to confirm that you are not impersonating someone else. You also cannot create an account for someone else unless they have given permission, in other words you cannot create an account for your child or another Individual, thus any accounts created to impersonate a celebrity are against the terms and conditions.
- Users are not allowed to solicit content to other users on the platform.
- Violation of the terms of conditions, including the encouragement of the violation of the terms and conditions, this includes the playing of copyrighted music, the bullying of other users etc. is against the community guidelines.
- You cannot post private or confidential information that violates an individual's rights, including their intellectual property.

How is this information used?

The information that is gathered is used to provide relevant content for the user in question, by looking at what the users follows, likes and information that has been provided by the user (including data with special protections which has been provided by the user) to help provide suitable suggestions for the user.

It should be noted that the information gathered from Instagram is not just contained with Instagram, but it also shared with Facebook, as Facebook is the parent company of Instagram and thus all the data is contained together, making it possible to be exchanged between platforms. I.E signing up with a Facebook account lets you have all your Facebook account information be default on the Instagram platform.

The information that is gathered from where you "check in" on the platform is used for generating suitable advertisements based upon places you go, this is done by gathering your devices location, however, can only be done if you allow the location to be accessed.

Information provided is also used in the furthering of research and development for the Instagram platform and its connected platforms i.e. Facebook, by conducting research and surveys and troubleshooting their new products and features.

They also use facial recognition software to recognise your face in photos and videos, however this feature is entirely optional and are considered special data under EU law.

What permissions you've given to Instagram:

When it comes to the ownership of an Instagram account, you have given Instagram certain permissions, these permissions are:

- Although Instagram doesn't claim ownership over your content, you do give Instagram license to use your content. Therefore, any content that you post, you grant Instagram a "Non-exclusive, sub-licensable, worldwide licence to host, use, distribute, modify, run, copy, publicly perform or display, translate and create derivative works of your content". Therefore, anything you post can be used for advertisements by the Instagram company at any time. The only way to end this license is through the deletion of your content or the deletion of the account the content is hosted on.

- Instagram has the permission to use your username, profile picture, likes and follows to post appropriate advertisements and offers, in other words, if you follow a sponsored content, you will appear on the advertisement about the content, with no compensation to yourself, this is however regarding the user's ad settings which can altered.

- The company can update your App on your device without permission.

- Instagram can change your username or similar identifiers of your account if it is impersonating someone else's identity or infringing someone else's intellectual property.

Removing content or terminating accounts:

- Any content that is deleted may still exist on Instagram for a period of time as backup copies and will be visible wherever others have shared it. This will still apply even after your account is terminated or deleted.
- Any content or information that is seen as a violation of Term of Use, or is illegal can be removed by Instagram, as a result they can refuse to provide all the services of Instagram, up to disabling or terminating your account. If your account is terminated you will be

notified, if you believed it is an error, you are able to make a counterargument to Instagram.

Who has rights:

- Third parties do not have rights under your agreement.

- You cannot transfer your rights or obligations to anyone else without Instagram's consent.

Who Is Responsible if Something Happens:

- Instagram says they can't guarantee their platform is safe and secure or that their security will work perfectly all the time. This does not exclude liability of death, personal injury, or fraudulent misrepresentation on behalf of Instagram's negligence, or if the law does not allow it.

- They also state that they have no control over the actions of other people, are not responsible for yours or other people's actions or content posted, they are also not responsible for services and features offered by other peoples or company, even if they were accessed through Instagram.

- Instagram is limited for what can be done on the service, due to the limitation of the law. any impact on issues pertaining to the service is unknown. And they will not be held accountable arising out of or related to their terms.

- Upon accepting of the terms, you agree to defend Instagram in any claims, liabilities, damages, losses and expenses against the company, for example, any attorney's fees and costs. You will also cooperate in defence of any claims and reserve the right to control any subject to indemnification, you will also not settle any claims without Instagram's consent.

How disputes are handled:

- Except as provided below, you and we agree that any cause of action, legal claim, or dispute between you and us arising out of or related to these Terms or Instagram ("claim(s)") must be resolved by arbitration on an individual basis. Class actions and class arbitrations are not permitted; you and we may bring a claim only on your own behalf and cannot seek relief that would affect other Instagram users. If there is a final judicial determination that any claim (or a request for relief) cannot be arbitrated in accordance with this provision's limitations, then only that claim (or only that request for relief) may be brought in court. All other claims (or requests for relief) remain subject to this provision.

- Unless in the exceptions below, any disputes between Instagram and you, based on the Terms of Instagram must be resolved by the use of an arbitrator or individually. Any class actions or class arbitrations are not permitted. You can only bring a claim on your own

behalf and cannot seek relief from other Instagram users, this rule also applying to Instagram.

- You or Instagram can also bring claims to small claims court instead of an arbitrator.

Data Policy:

It is detailed within the Instagram data policy that they collect specific data, depending on how you use the product. However, you do have the ability to view, download and delete said data from their servers.

What is collected:

Data provided by the consumer:

- All created and shared content by the users.
- Messages and communication with others.
- Location of the photo (if provided).
- Date of file created.

Network and connections:

- Collect data on pages and people followed.
- Pages and people that follow you.
- Hashtags you follow.
- People you communicate with.
- The messages sent to these other people.

What data is collected for:

- Login activity.
- People you have searched for.
- People you have interacted with.

- Time, frequency and duration of your activities.
- Content you viewed.
- Features used with the camera.

What is shared with Third-Parties:

Instagram (and Facebook) work with a lot of third parties in order to be able to provide the free service that they do, even though they impose strict restrictions on how their partners can use and disclose the information they provide. Below is a list of information that Instagram shares with their partners.

Analytics:

Instagram provides companies with statistic to help companies understand how users are interacting with their posts, listings, pages videos and other content. One way being Instagram business profiles receive data on how many people view, react and comment on their posts.

Advertisers:

Instagram provide reports to advertisers to see the kinds of as people are seeing and how their own ads are performing. However personal information is not shared with these companies. Unless permission is given to do so.

Measurement partners:

Instagram shares your info to companies in order to provide analytics and measurement reports to their partners.

Service providers:

Instagram provides information to their venders and service provider who support their business, by providing Instagram with a technical infrastructure service, analysing how their products are used, provide a customer service, conducting surveys or facilitating payments.

Researchers:

Instagram provides your information and content to their research partners in order to further their research, that is used to advance scholarships and innovation that supports Instagram (and Facebook's) mission. Enhancing the discovering and innovation of technological advances, social welfare, health and well-being and public interest.

Legal requests from law enforcements:

Instagram is by law, obligated to share your information with law enforcements in the case of a legal case.

Your rights under GDPR:

Under the General Data Protection Regulation, you have a right to access, rectify and erase your data, you also have the right to restrict the processing of your data:

- You have the right to object of the processing of your data for the purpose of marketing, this right can be exercising by using the "unsubscribe" feature on marketing communications, like at the bottom of emails.

- You have the right to objectify against the processing of your data where it is being performed in the interest of public interest or in the interests of a third party.

Account deactivation, deletion and data retention:

Instagram and Facebook stores data on their servers until that data is no longer necessary in order to provide a service on their services, or until you delete your account. However, this also depends on the nature of the data, why it was collected and how it was processed, and the legal or operational retention the data is needed.

When you delete your account, all the content you've posted, like photos and statuses will be deleted, and will not be able to be recovered later. Content that others have shared about you however will not be deleted due to it not being your data. If you want to get rid of your account but keep your data on the service, you can deactivate.

Responding to legal requests:

As previously mentioned, Instagram will share your information to law enforcements, regulators etc. for the following reasons:

- Instagram will send your information in response to legal requests when they have a good-faith belief that it is required by law in the jurisdiction the request is being made place, and it is also with consistence with the international standards.

- With the good-faith belief, it is necessary to detect, prevent and address any fraudulent, unauthorised use of Instagram, in regard to violation of their terms and policies, or any other harmful or illegal activity, in order to protect the service, yourself and/or others.

Community Guidelines:

Only share photos and videos that you have taken or have the right to share.

As always, you own the content you post on Instagram. Remember to post authentic content, and don't post anything you've copied or collected from the Internet that you don't have the right to post.

Only post content appropriate to a diverse audience.

Instagram does not allow nudity on their platform, however post-mastectomy scarring, and women breastfeeding is allowed. Pictures of nude painting and sculptures are allowed though.

Any pictures that contain nude or partial nudity of children will be removed from the service entirely.

Foster genuine and meaningful interactions:

Don't spam the platform by artificially getting likes, followers and/or shares, or by posting comments or content repetitiously, or by repeatedly tagging users about products without their consent.

Follow the law:

Instagram does not condone support for terrorism, crime or hate groups, the offering of sexual services or the selling of illegal firearms or prescription drugs. Any accounts that promotes online gambling must have written permission before using Instagram.

There is also a zero-tolerance policy on the sharing of sexual content involving a minor and threatening to post intimate images of other people.

Respect all members of the IG community:

It is against the rule to published threatening messages or hate speech, content that targets private individual by degrading or shaming them. It's also against the rules to encourage such violence or attacks based on someone's race, nationality, ethnicity, origin, sex, gender, gender identity, sexual orientation, religious affiliation, disability, or disease. Serious threats of harm are also not allowed.

Not glorifying self-injury:
Instagram does not condone the encouragement of people causing self-injury such as promoting eating disorders, cutting and other types of self-injury. This might include newsworthy events, depending on how graphic the images are.

Regarding Reporting Content/Users:
If there is a violation on the platform than Instagram recommends the use of the reporting option on the platform, to remove such content to keep the community clean, individuals can also report an account without having an account. They do request to provide as much information as possible like links, usernames and descriptions of the condemned content, as to speed up the review of the content. However, if you find content which you just don't like and doesn't violate the Community Guidelines, they ask not to report this content, but just to block or unfollow the user who has posted it.

They also insist that if there is a dispute or misunderstanding between two users which is not a violation of the terms of service or the Community Guidelines, that they resolve it between each other. Posting screenshots and drawing attention to the situation may be classified as harassment.

Lastly, they insist that they will work with police enforcements if there is a risk of physical harm or a threat to public safety.

All the above has been condense and abbreviated however, the original source material pertain to the terms of service **Instagram (2019)**, the data policy **Instagram (2019)** and the Community guidelines **Instagram (2019)**, in their original legally binding format, on The Instagram website.

11.2.2 Instagram Features

Instagram is a content-based platform, in which users can post photos and videos to the platform. Comments can be placed on content users have uploaded. Instagram allows the use of private messaging, content can be deleted after it has been posted, it is also able to be archived, so a user can re-upload it later. “Follow” is very similar to friending a user on any other social media platform, in which the user can access the “followed” users’ content, which the followed user has allowed to be accessible. All the content from followed users is accessible via the timeline section of Instagram. The user is also able to see the activity of any followed users by accessing the “followed” section. The user can also use the internal messaging service, users may also share content posted by either themselves or other users, if those contents can be shared. Another feature of Instagram is Instagram TV service, in which a user may share video content directly to the public platform.

Instagram allows users to post content, that is only available for 24 hours, known as “Stories”, one of these features is the ability to livestream on Instagram. Instagram also facilitates advertisements on the platform, that appear on the user’s timeline.

Instagram allows a user to be able to search for other users, using the search feature. Inside of this feature also have several recommendations for the user to follow.

As of March 2019, The Facebook company is planning to add end-to-end Encryption to the Instagram Instant Messaging services, stating that it is a priority for 2019, and plan to be released by 2020. **(Zuckerberg M. 2019)**

11.2.3 Instagram’s Personal Security Optimization Options

Instagram offers the following settings:

- Manage Privacy Settings
- Manage comments on your content
- Manage who follows you
- Manage who messages you
- Manage users (Block, Report)
- Manage who can see your story (And who can share it)
- Manage inappropriate advertisements
- Manage the Geo-Location to photos

In the section below, we will detail how these features can be performed.

11.2.4 Instagram Settings

It should be noted that any content that is posted, is available to be seen publicly and can be viewed by other users at their own discretion, unless you have set your account to be private, giving you the ability to choose who can follow your account.

To further explore these features, we created two accounts, one under the age of 18 with the user handle “iamanexample_username”, this account will allow us to see how Instagram reacts to a user who is underage, and a second account over the age of 18 with the username “exampletwoelectricboogaloo”.

As previously mentioned, all accounts come with the ability to enable a privacy setting that, when enabled allows you to choose who can view and follow your content.

This feature can be enabled by going into the settings feature on the users account page, and scrolling down until you find the option for “private account”

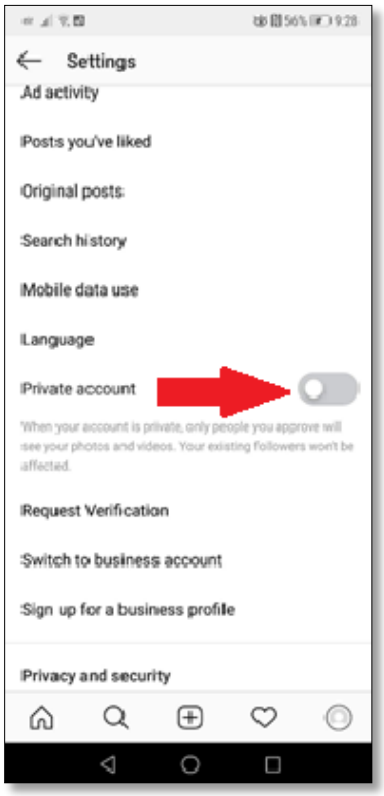


Figure 78 Private account toggle switch.

By default, any information you have shared, is not downloadable via the Instagram platform, however, there are several methods that can get around this restriction by screenshotting the image, using third party applications, etc.

There is also a feature to allow for a user to find relevant content depending on their likes and the follows the user has. This content is available to anyone (if the profile is publicly accessible).

This can lead to the possibility of the user’s content being found depending on which tags are added by the user to their submitted content or by searching for the username of the user, meaning anyone can find their content depending on their privacy.

There is also a content channel feature known as Instagram TV, or IGTV, which allows for 10-minute videos to be recorded, or 60 minutes if you are verified or popular, this can be found at the top right of the timeline section, this feature is only available on mobile phones and cannot be found on the desktop version.

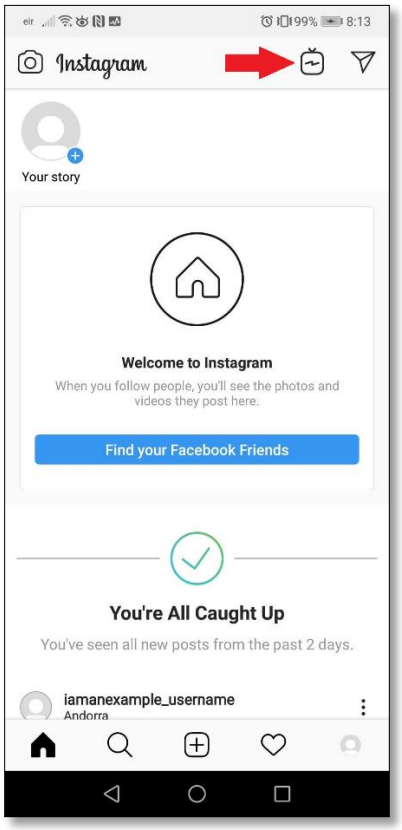


Figure 79 The button where Instagram TV can be accessed.

Multiple videos can be posted on this platform, and they are not deleted after a period. Anyone who has an Instagram account can set up a channel to broadcast themselves. There is also a social aspect to Instagram, in which you can comment, tag people so they can also see a photo, and privately message some people.

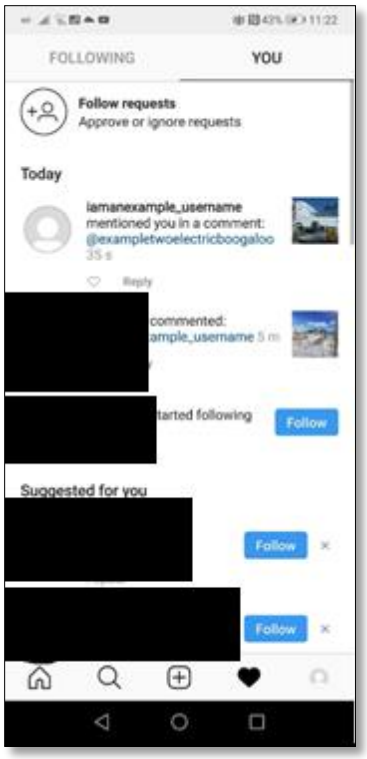


Figure 80 A user being tagged in a photo.

When it comes to commenting on content, if your account is not private then anyone can comment on your photos and tag others to view your photo, however if you have privacy enabled, only people who you have allowed to view your content. By allowing them to follow your account, users can comment on your content, if they tag a user who is not following you or you have not allowed follow you, they will not be able to see that they have been tagged nor be allowed to view the content.

When users comment on your content, if you find that someone has commented in a manner which you find inappropriate, you have the option of deleting that person's comment; by holding down your finger on the comment in question. You will be prompted with the ability to delete that user's comment.

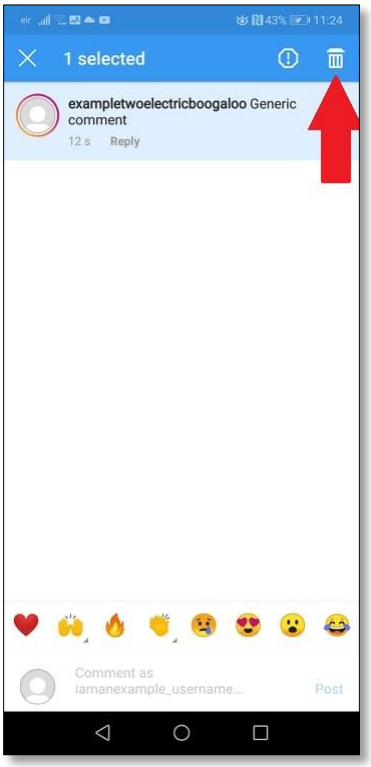


Figure 81 Deletion of a comment.

When it comes to followers, anyone can follow your account if your account is public; however, if your account is private, they must request to follow your account. If you delete the follow request, the user can still request to follow again for an unlimited amount of times, however that can be remedied by blocking the user.

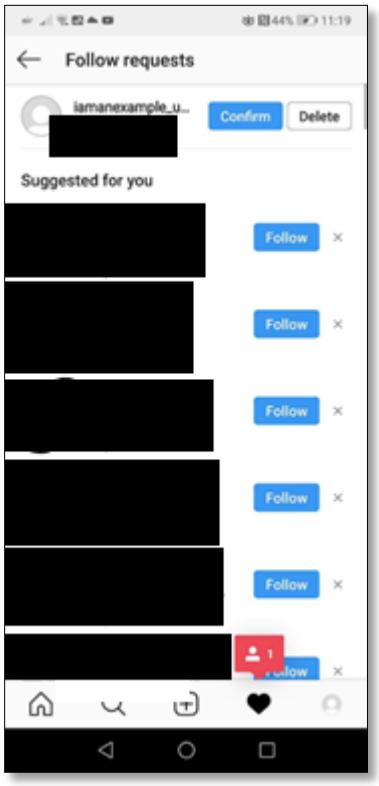


Figure 82 A follow request.

Regarding messaging on Instagram, anyone can contact the user, regardless of their privacy settings, however the user has the choice of whether they want to converse with another user who they are not following. If they allow the other user to contact them, then they'll have full ability to contact them via Instagram at any time, however this does not mean that the user is able to view their content if their content is private and they are not following them. the user will also still be able to block the other user if they feel they need to.

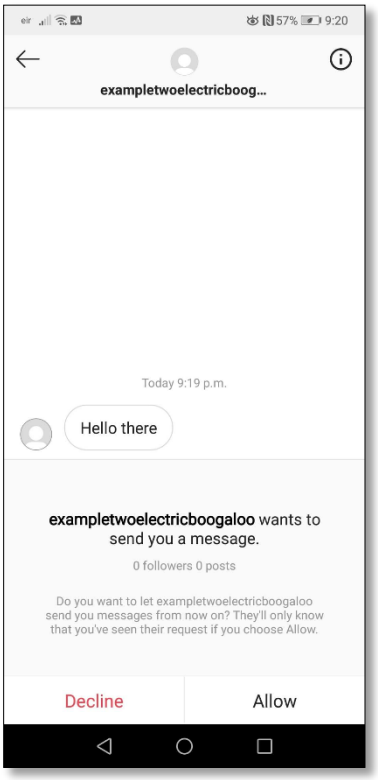


Figure 83 Here, the user has received a message request from another user, which will allow the unknown contact to communicate with the user.

However, if the user declines the message then the other user's message will be deleted, and they will be unable to contact the user anymore unless you initiate contact, or they are followed. This feature can still be abused, where if an inappropriate message or photo is sent, it is still viewable before it is declined. This can be several photos and images If the user has sent a message, that they'd like to unsend, they have the option to unsend that message by holding down on the message and selecting "Unsend message" from the prompt that appears. This will also cause the message on the side of the other participant to also be deleted as well, which is advantageous compared to other social media Apps where the message is only deleted on your side, this feature also works the same way in a group chat.

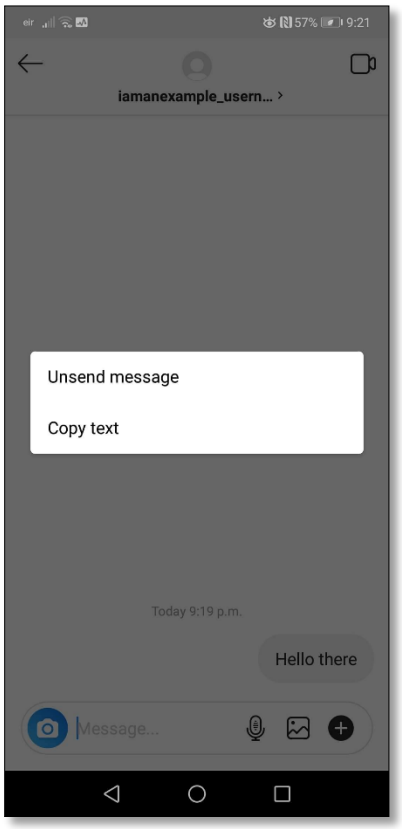


Figure 84 Here, we see the user about to unsend a message that was previously sent to another user.

This can be useful for a parent, where if a child gets access to the parents account and starts typing inappropriate content onto a chat, the parent could delete that content. However, there is still the possibility of the content being seen on the other end before it has been deleted.

For whatever reason there may come a time when you wish to block another user. This is easily done, by going on the user's account to be blocked and going into options on their account (the three dots on the top right for Android devices) you are prompted with option an option to block the user. You can unblock the user if need be by going back to this options menu and unblocking them.

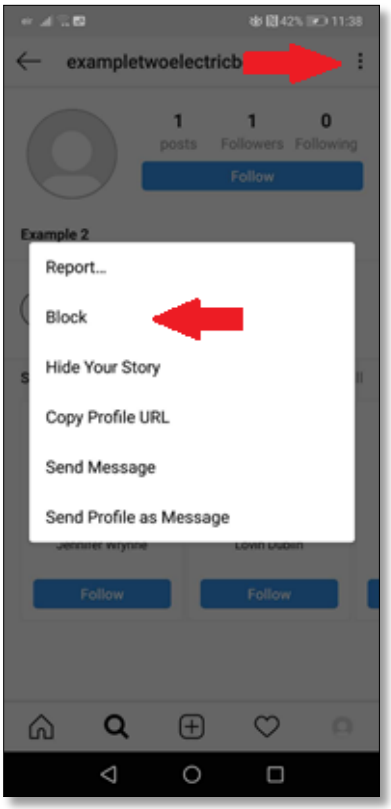


Figure 85 Here, we see the user about to block another user.

When that user is blocked, they are unable to view your account or any of your content or see any of your activity on the platform such as comments. Another feature that is also available is the report an account feature, when you report an account you are given two types of options to report it as, the first is reporting the account as spam, and the other is reporting it as inappropriate content.

Users can share pictures and videos for a 24-hour period, known as stories, these stories are accessible on user's page, or on the timeline. From this section you can host live streams, which is represented by a red ring around the story bubble, with live on the bottom of it. Anyone may be able to access the live stream, depending on your privacy settings.

Figure 86 Here we see were the story option can be accessed.

In this section, anyone who is viewing the live stream can comment and react on the live stream, which the user can view and react to.

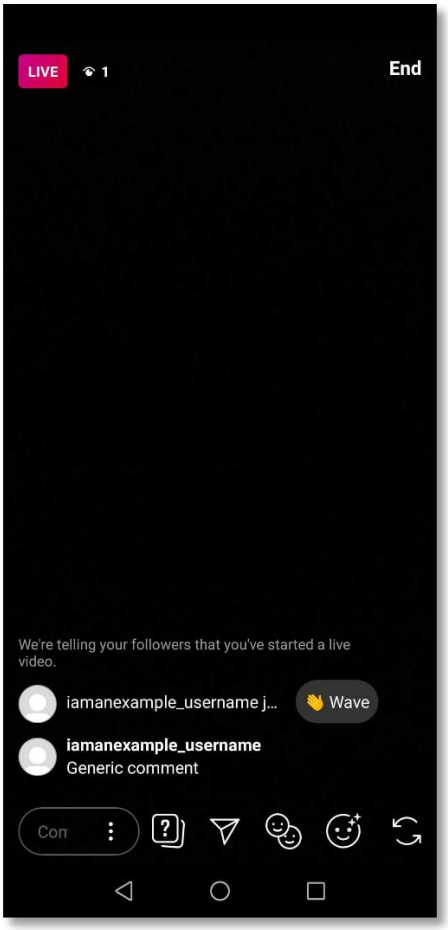


Figure 87 An example of a generic comment on a live stream.

In a user's story, the owner can set who is able to view their story, choose who is able to share the story to their friends, and choose who can message you from the story image.

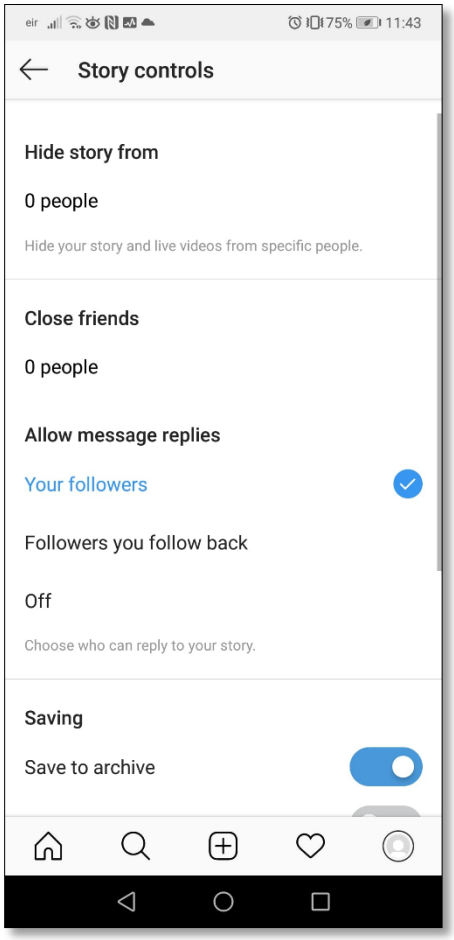


Figure 88 Story Controls.

You also can block someone from seeing your story entirely. This feature can be found in the in the same menu as the previous selection. When you report an account, the information is reviewed by the Instagram moderation team in conjunction with the community guidelines, and the account receives a warning. On the second report, should the report be found valid, the account is deleted. The reported account is never informed on who filed the report, leaving the entire report entirely anonymous.

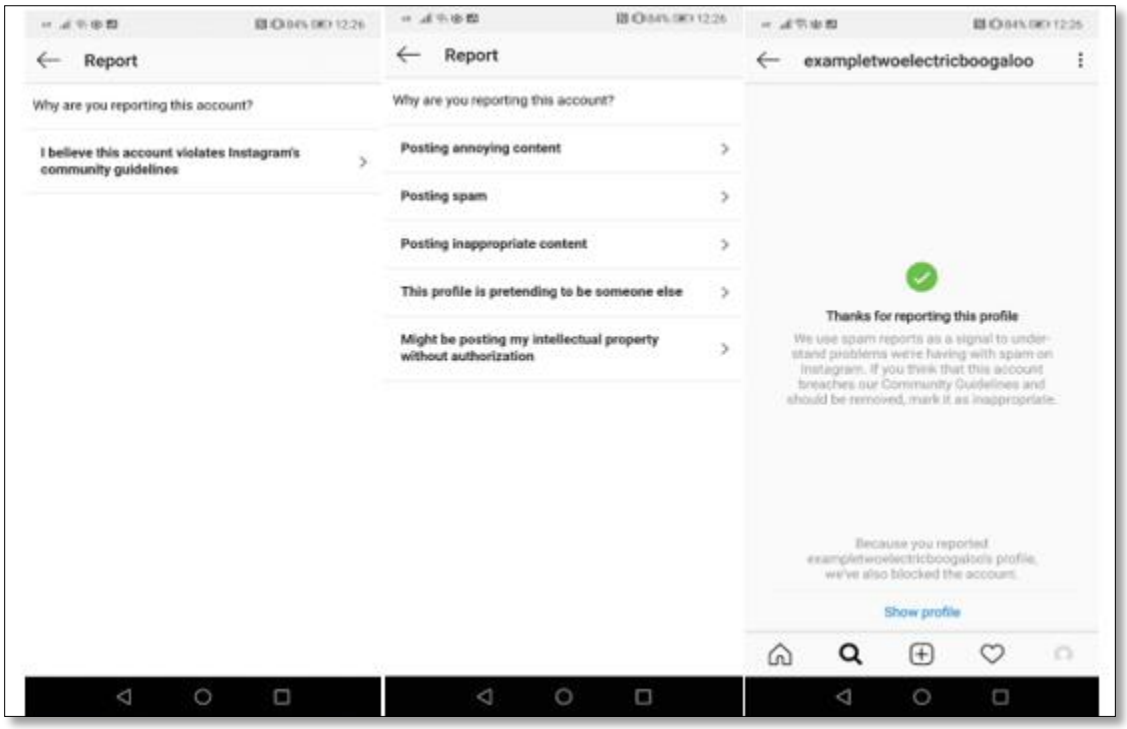


Figure 89 From left to right we can see the sequence of the reporting process

An option that is restricted to private accounts is the ability to make followers unfollow you, it can be accessed by going onto your followers' section and selecting the options buttons beside the user you wish to unfollow your content, giving you the option to make them unfollow you. They will also not be informed that you've made them unfollow you and will only notice if they make their way to your page.

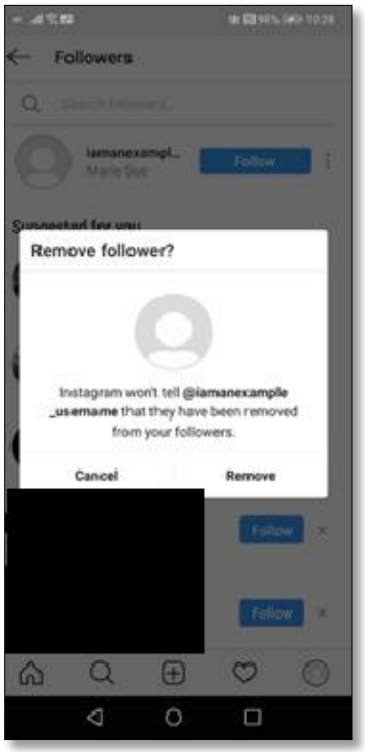


Figure 90 Here we can see a user being unfollowed.

Meta-data is used to decide what advertisement are shared on an Instagram feed. However, when it comes to children under 18, there is an option to ask a parent for the allowance of data gathering. This is a due to an US law known as Age-Gating, in which Instagram will automatically make you unfollow brands and make you unable to follow them, until the legal age is met.

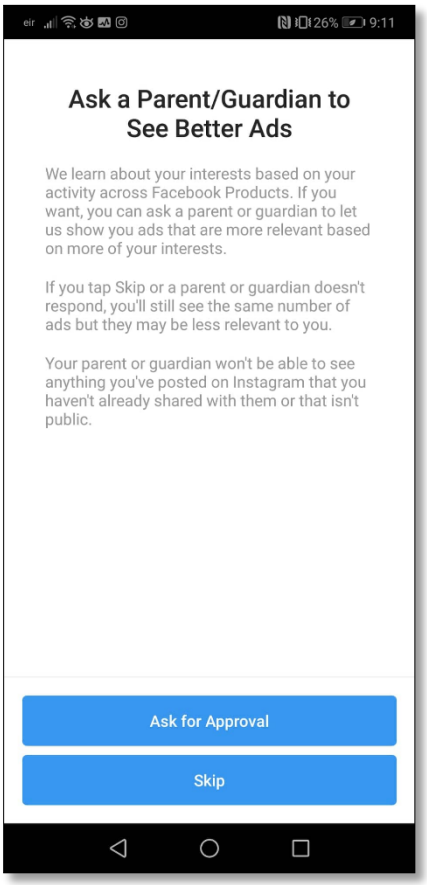


Figure 91 Instagram requesting the permission of a parent or guardian in the relation of showing ads.

This can be skipped, giving no option to return to this option page.

If you see an advertisement you don't like, you are able to hide the ad by selecting the option on the side of the picture (the three dots), asking why you hid the ad afterwards, to try improving your ads on the platform.

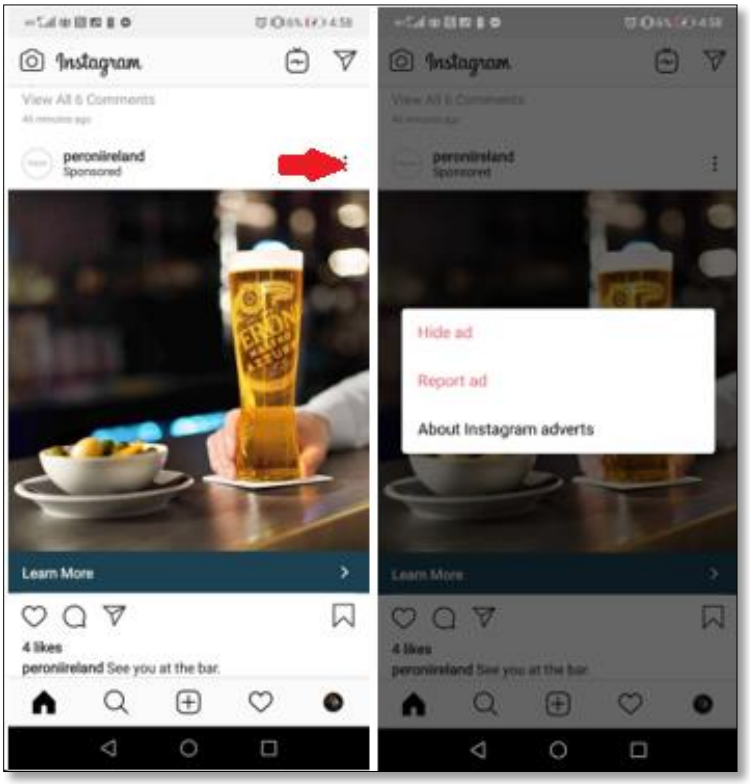


Figure 92 The act of hiding or reporting an advertisement.

All users can archive data, by selecting the options section on the photo (the three dots), you are presented with a menu in which you can archive the photo. This can be very useful for photos that you wish to get rid of for a select amount of time.

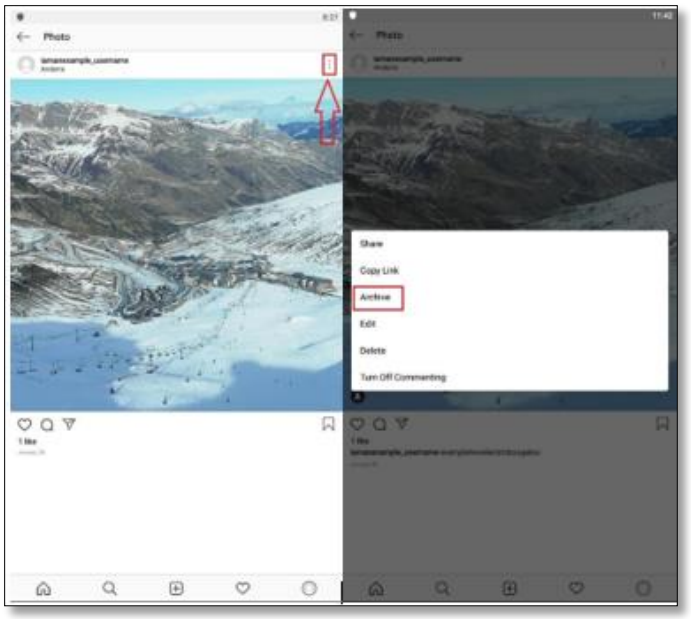


Figure 93 The user in the process of archiving content.

There is also an ability to view all previous stories that have been posted on the account, this can be done by pressing the timer icon on the top of the user's profile. There are two archives in this area, Post Archive and Stories Archive, from stories archive you can see old story posts and if desired, repost them to your story. On the posts archive, you can access any photos in which you have archived, and if desired, can have these photos reappear on your timeline. You can change between the two archives by selecting the archive name on the top left and choosing between the two.

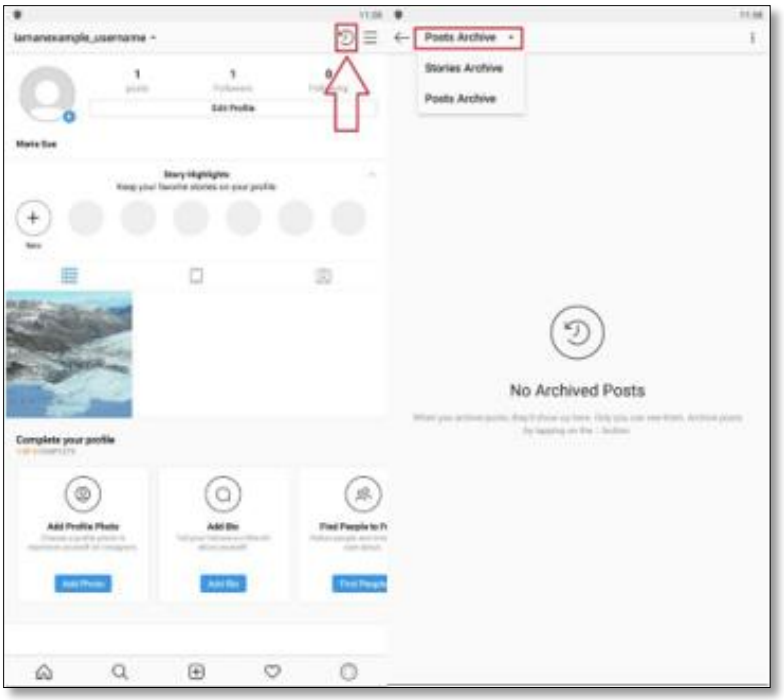


Figure 94 The process of retrieving achieved content.

All the user's data can be accessed by the user and downloaded. This data contains all the name changes, message logs, photos, videos, searches, previous and current profile picture and stories. When you request these, Instagram asks for your email and sends you all your information within 48 hours that you can look through. This feature can be accessed via desktop or by the App.

Figure 95 A user about to retrieve their own content.

We tested this feature by having requesting information from a personal account, the result was that we received an email a few minutes later with a zip file containing a large amount of information about the account. All the information is stored within .json files, and as a result is best opened with a computer. These files can easily be opened with a text editor.

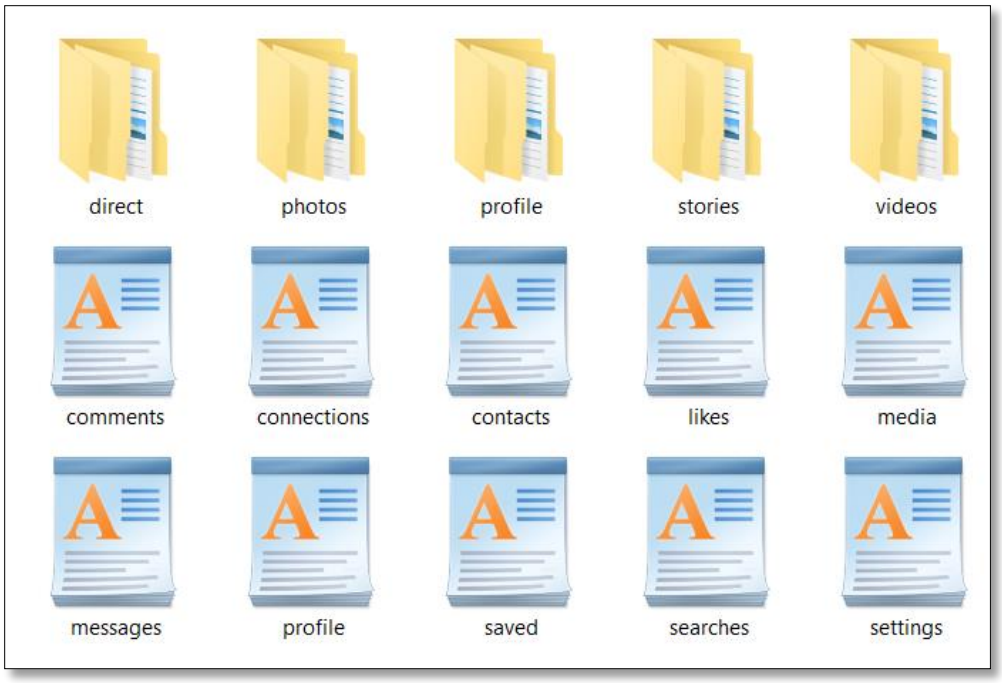


Figure 96 All the folders and files which are sent to the user because of retrieving data.

All this data can be accessed without downloading it, by going into the settings, privacy and security, Access data. This allows you to view all the data that could be downloaded without having to.

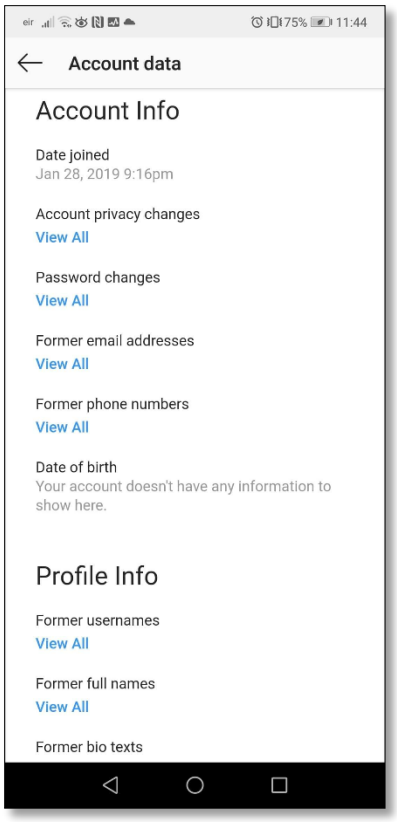


Figure 97 This section allows for a user to view all their data that Instagram stores.

When it comes to reducing your footprint, most settings can be accessed by going into settings and selecting the privacy and security option.

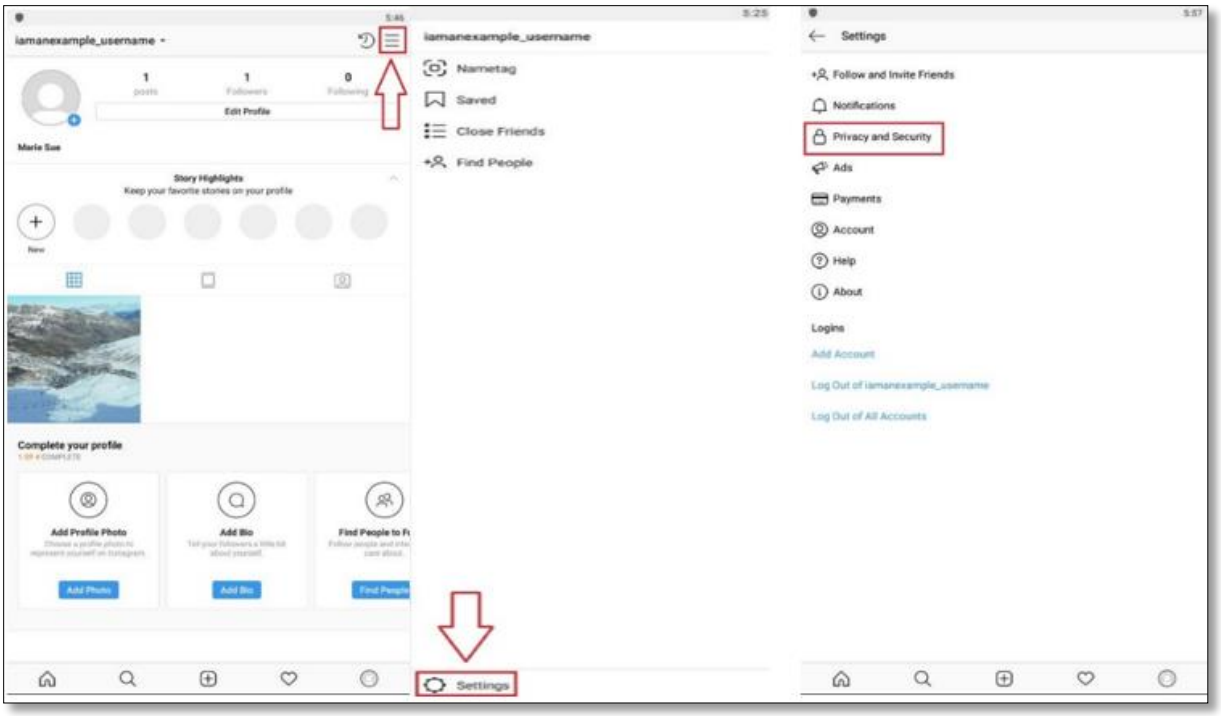


Figure 98 From left to right, accessing the privacy and settings option.

From here you can enable Private mode, which prevents people from viewing your profile if they are not following you. This setting can be accessed by selecting account privacy within Privacy and Settings and enabling within this setting.

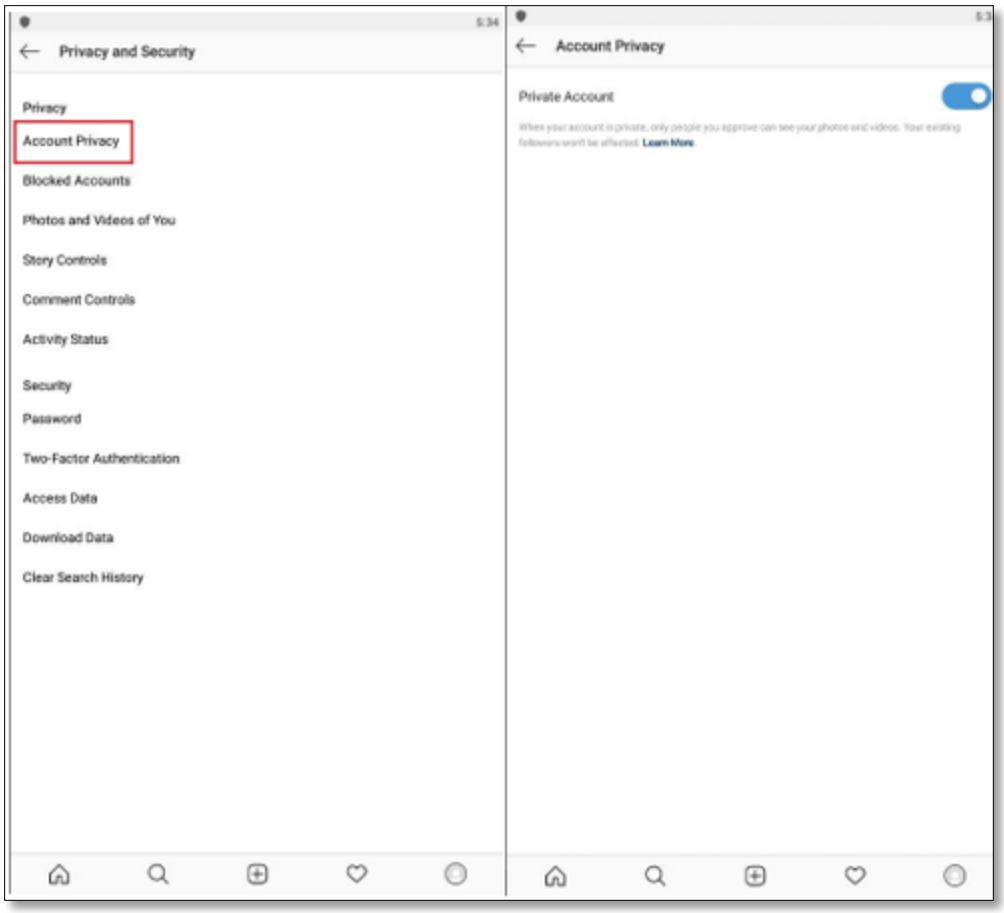


Figure 99 Implantation of private mode in the Account Privacy section.

After this is the ability to disable or remove photos which will appear on your account from other users, this can be done by entering the “Photos and Videos of You” section within Privacy and Security.

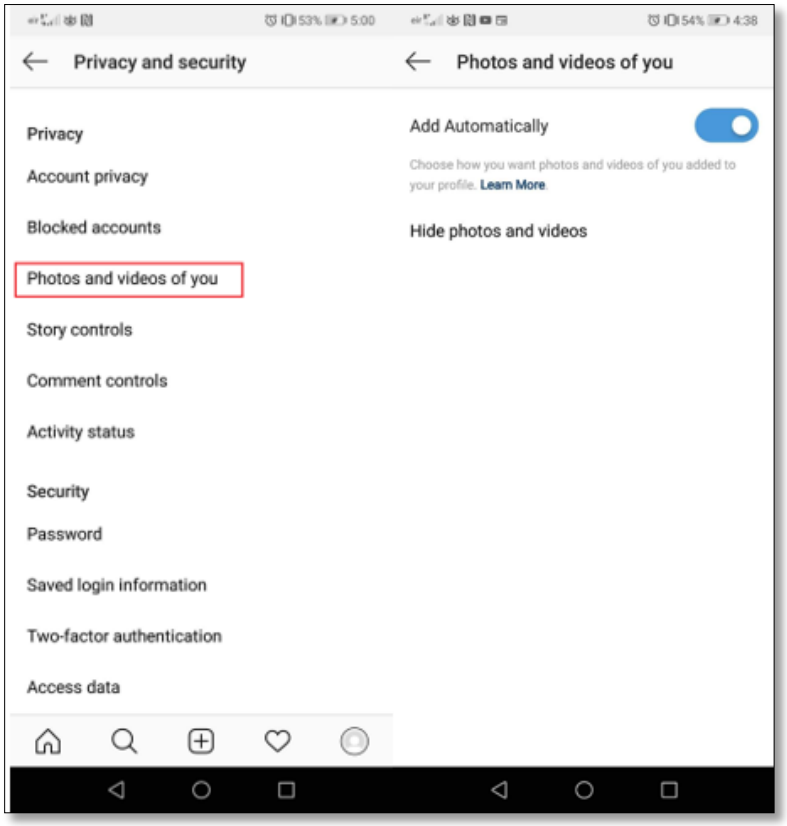


Figure 100 Here we see the option to toggle automatic adding of photos you are tagged in and the ability to hide said photos.

From this section you can disable the feature of having photos that are tagged with the user to be added automatically, you can also hide particular photos or videos within the section that are deemed unsuitable by the users. After this it is suggested to reduce who can see your story to certain individuals, as ensuring that you know who is able to see such content, this can be done by going back to the Privacy and Security settings and selecting story controls.

Preventing the ability for your story to be shared is also a good idea, as is preventing your story from getting sent to people you do not know. This feature can be accessed in the Privacy and Security settings, and selecting Story Controls, in this area under the heading “sharing” you are able to disable “Allow Sharing”.

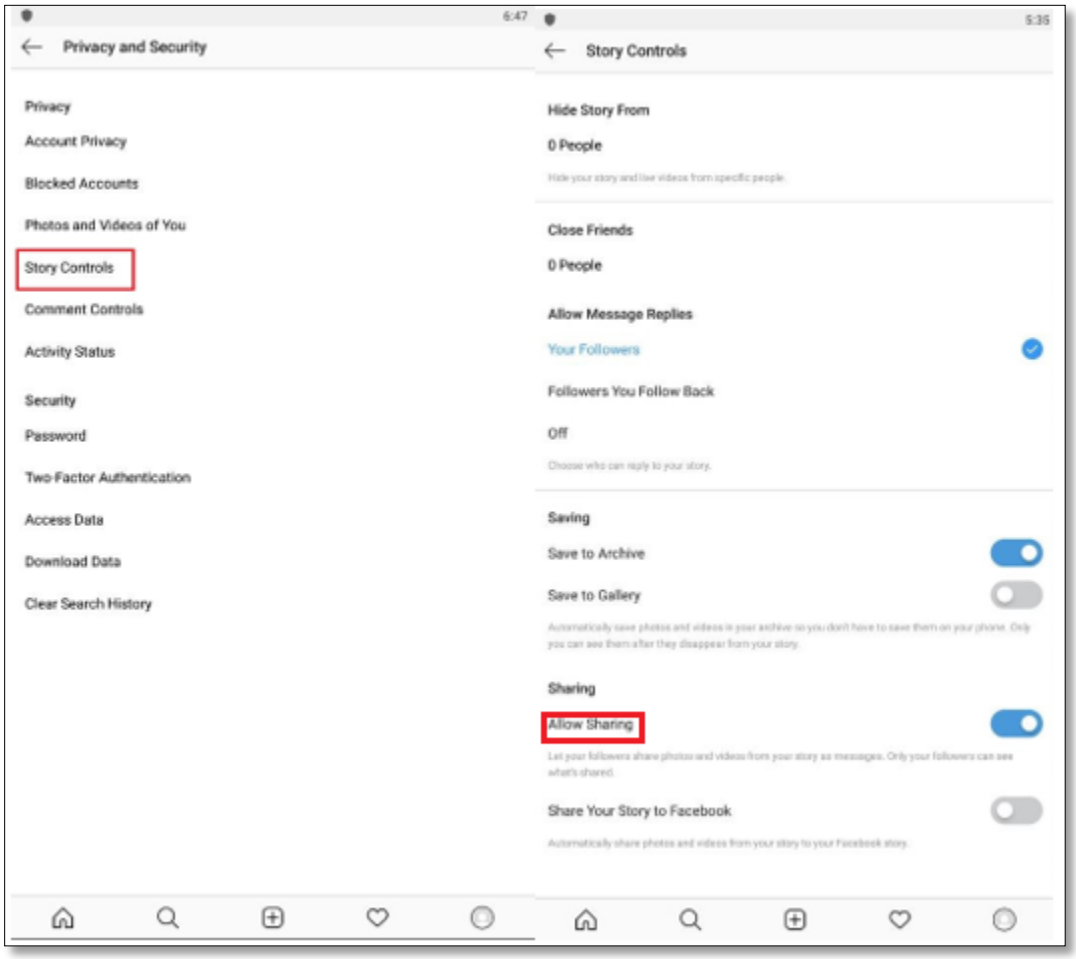


Figure 101 Accessing the story settings on the Instagram app.

With this, there is also the option to disable your story from appearing on your Facebook story (if you have a Facebook account connected) within the Story Controls, just under the Allow Sharing function. it is automatically disabled.

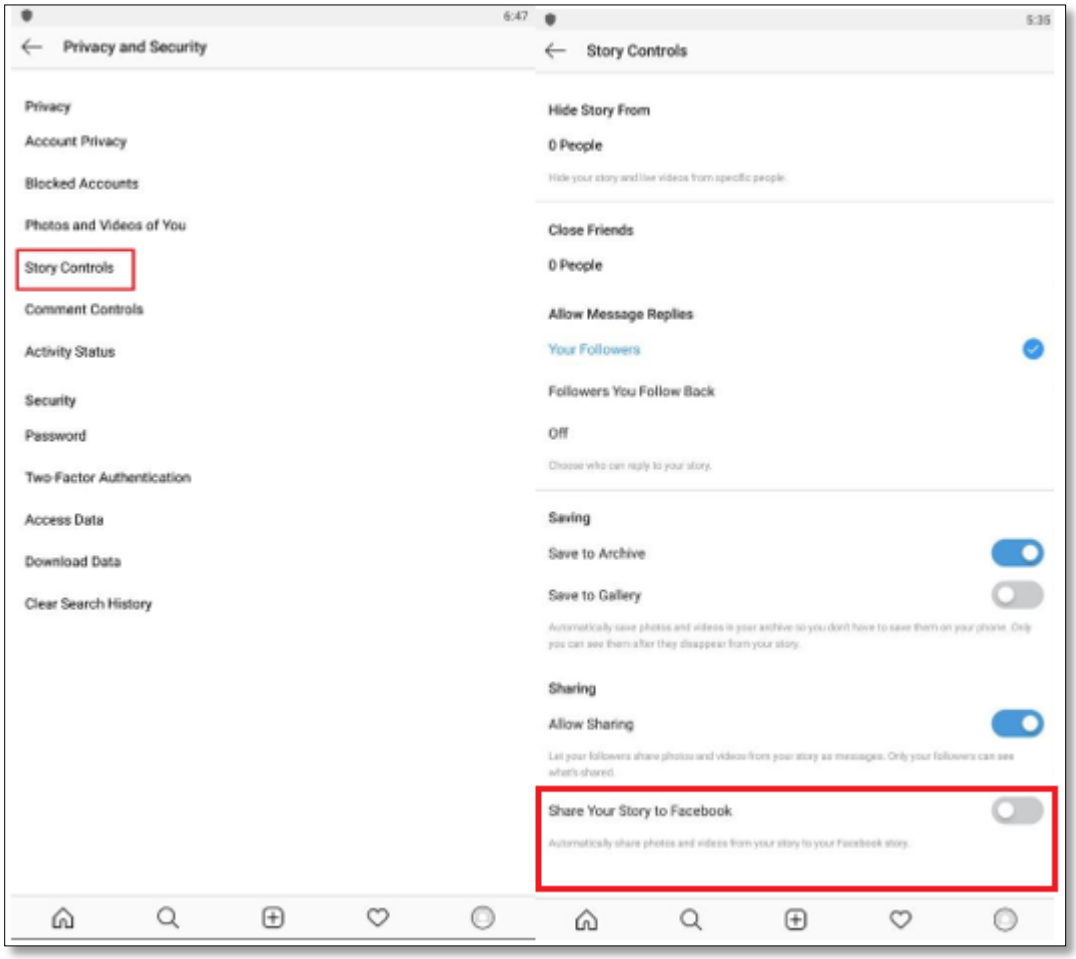


Figure 102 The toggle to automatically share your story to Facebook.

Within the Story Control settings, there is an option to choose who can message the users about their stories, this can be set to either to only allow your followers to contact about it, your followers who follow you back, or set off the messaging about stories entirely. By default, this setting is set to only followers.

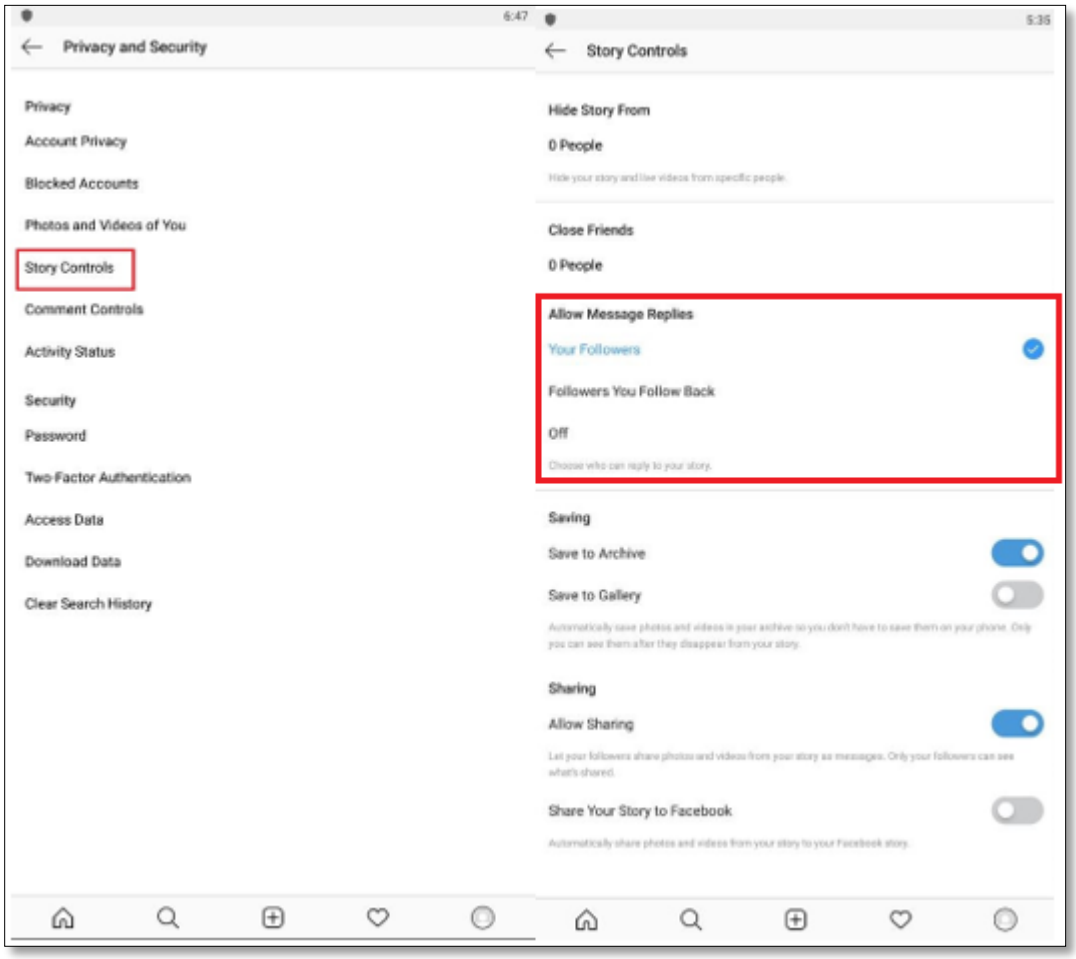


Figure 103 Here we see the option to choose can reply to stories.

There is also a feature to be able to hide your story from user within the Privacy and Settings section, this can be done by selecting the People, and selecting their name to block. This feature can be especially useful in blocking people from your story, but not wanting to block them entirely.

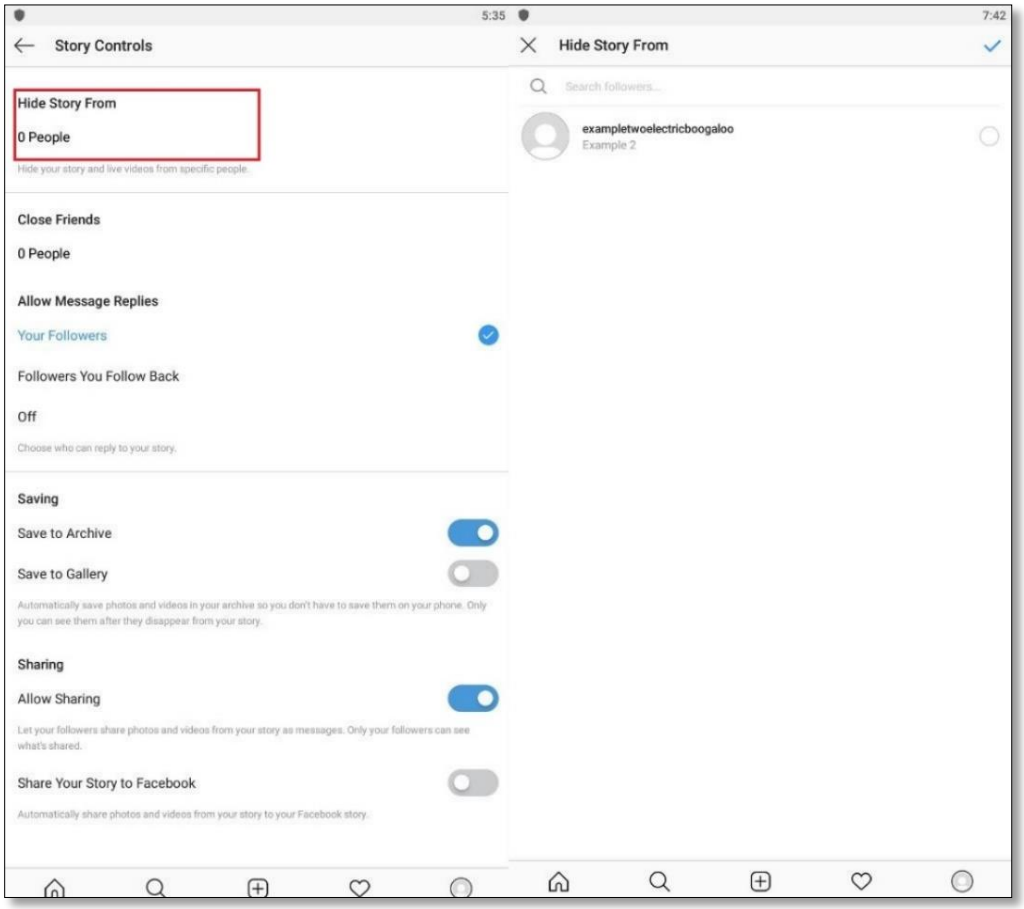


Figure 104 Here we see the option to hide your story from people.

On the opposite side of this, there is a feature to add users to a section known as “Close Friend” , this section where you can post separate stories for certain people, this can be accessed on the Story Control pages, people can be added by selecting them from the menu, or searching for them within the build in search function.

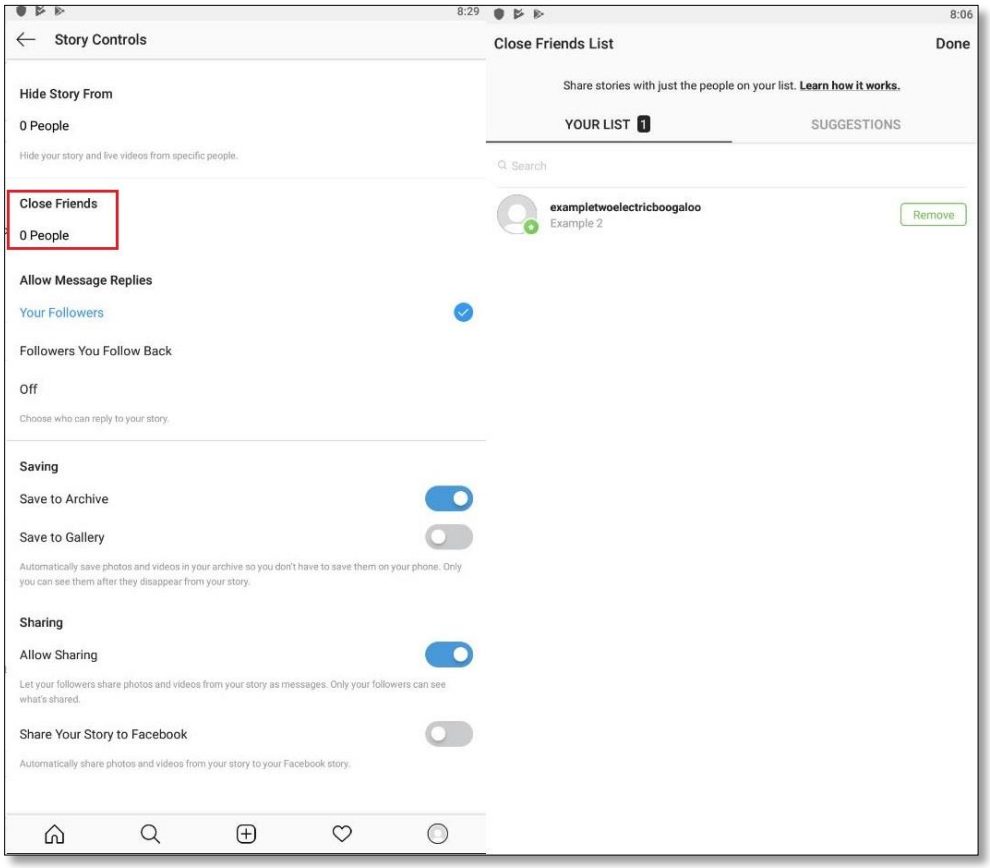


Figure 105 Here we see the option to add users to a close friends list.

The next feature in the Privacy and settings is the Comment Controls settings, within these settings is the ability to filter any offensive comments that is deemed unacceptable.

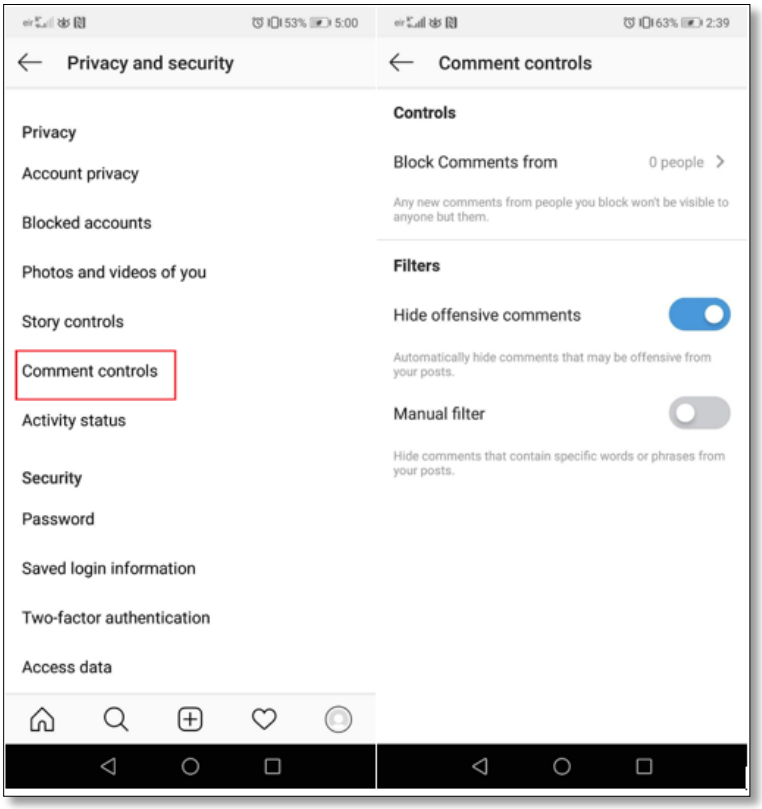


Figure 106 Here, we see the comment control settings on the left and the hide offensive comments filter toggle on the right.

From the comment control settings, you can block people from being able to comment on your content, without blocking them from viewing the content. You are also able to apply filters to what comments can be seen from the account, there are two settings that allow this. The first being the hiding of offensive content, that will block any content that could be offensive. The other is manual filtering, which allows the users to block certain types of words from appearing. This feature is most effective in combination with the filtering of Offensive Comments setting enabled.

Talking about the blocking of users, if you have already blocked a user, you are able to unblock users within the “Blocked Accounts” section.

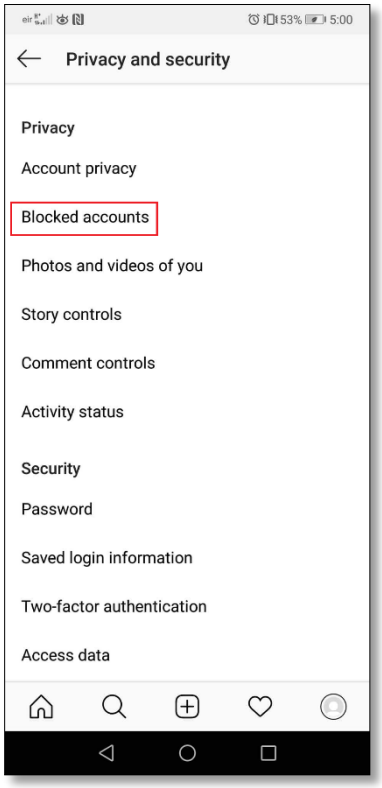


Figure 107 Here we see the feature which allows the unblocking of blocked users.

The next feature within the privacy and security settings is the activity settings, this setting, when activated will allow other users to see your activity. By default, this feature is set to active, so it will show all activity. You can disable it within this section. With it disabled, no one will be able to view your activity.

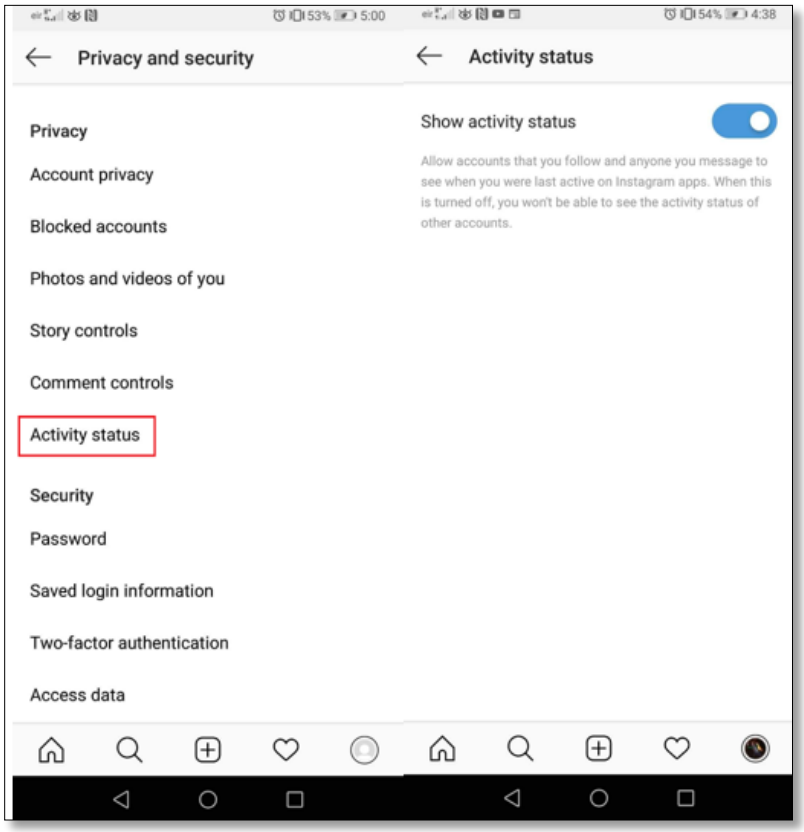


Figure 108 Here we see the activity status toggle which, when activated, will allow users to see your activity statues. toggle off to be invisible.

If there ever comes a time in which you have decided to change your password, you are able to do so by selecting the password button within the Privacy and Security section. This can be particularly useful in scenarios where you feel your account has be compromised.

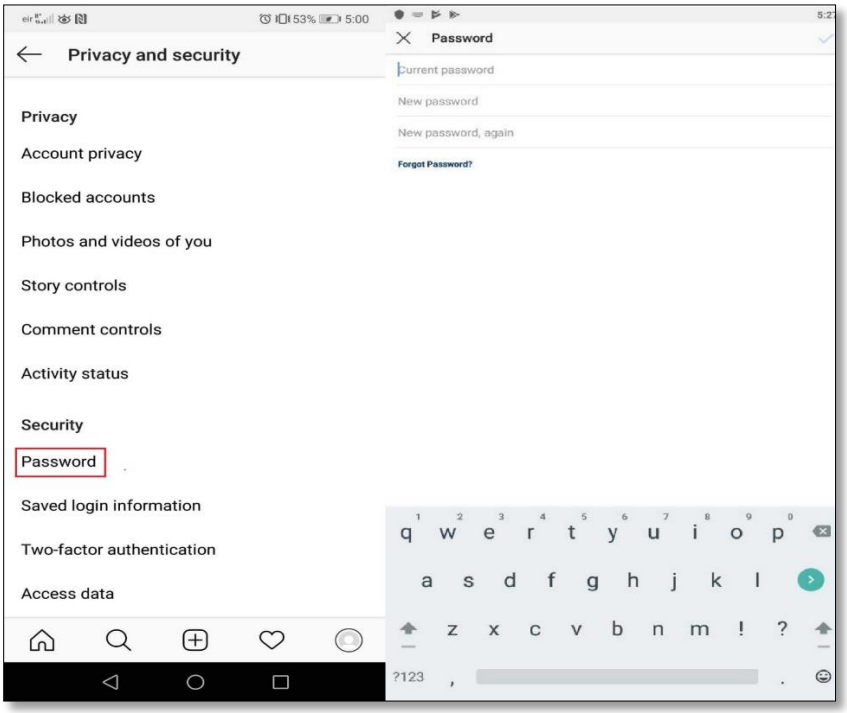


Figure 109 Here we see the section for changing the password to the Account

Within the privacy and settings section, you can enable two step authentications. There are two types of authentication that the App allows you to implement, the first being that you will be sent a code via text message if there is a login attempt from an unknown device. The user will have to enter the code to be able to access the account. The second type of two-factor authentication is that you are asked to download the Authentication app, that every time you try log in, it checks if the Authentication app. If you do then it logs in to your account, if not then it asks you for a code from the Authentication app.

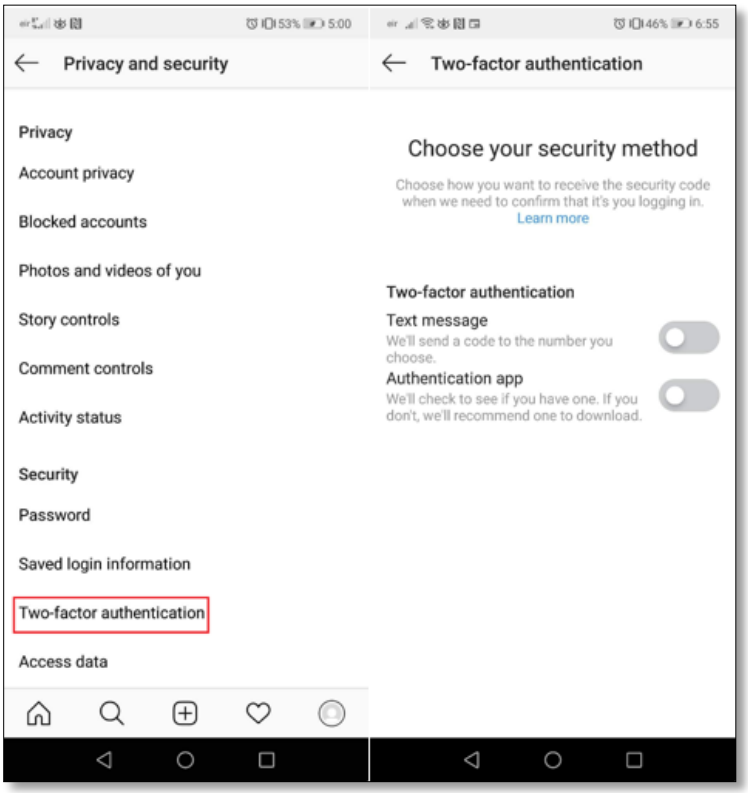


Figure 110 Here we see the option menu for the Two Step Authentication menu.

After initialising either one of the Two-factor authentication, you are presented with several recover codes in case you have lost your device and are unable to get into your device with the app. These codes are not reusable, but new codes can be acquired. however, it is suggested to screenshot these codes and store them on another device to be able to use these codes properly.

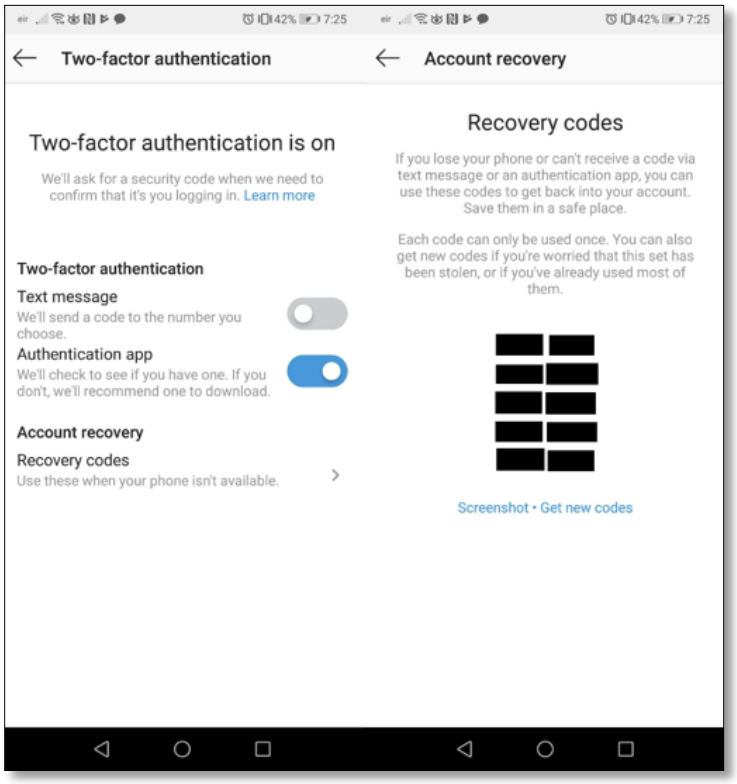


Figure 111 Here we see the recovery codes that are available after setting up a two-factor authentication.

Within Instagram, you can pay for goods and services through the app, with this there is a feature to add an ability to add a payment option. This feature can be accessed within the settings of the app. Within these settings is the ability to establish which methods in which you can pay for services.

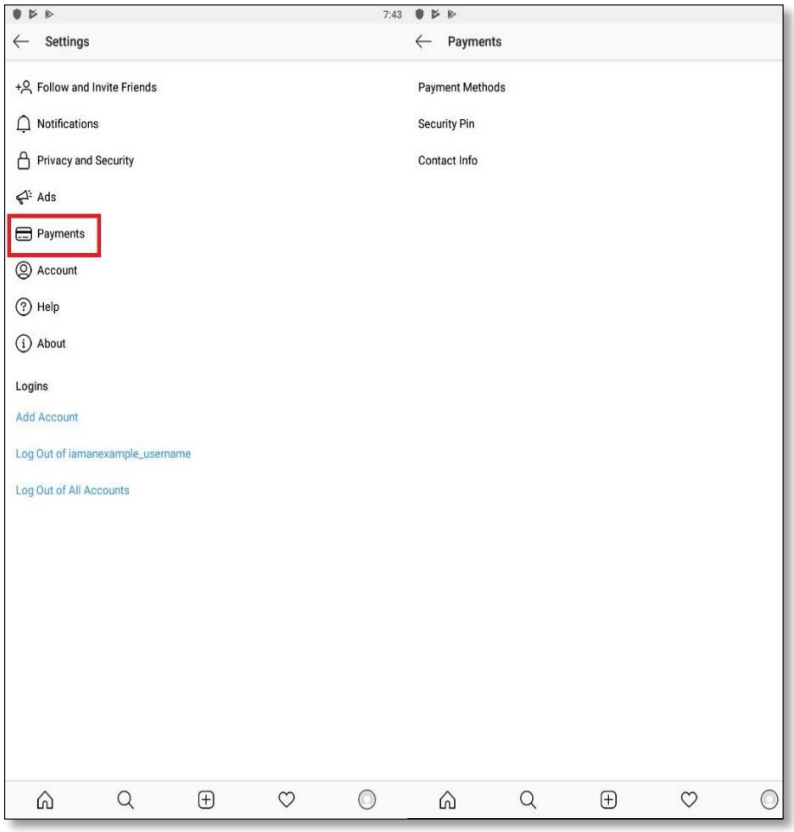


Figure 112 Here we see how a user can access the payment option on the App.

From this setting, you can set up a payment type on your account, this can be done by entering payment methods option and entering in your card details.

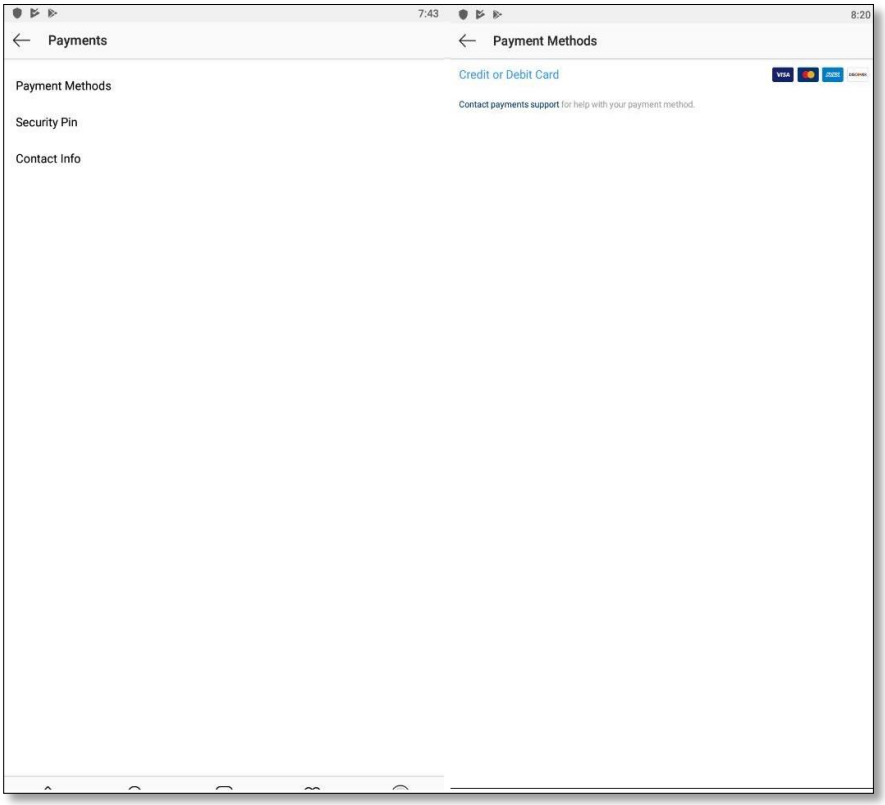


Figure 113 Here we see the setting to add a payment option to your account.

Within these settings you can set a pin on the account for every time there is a purchase. This is to prevent any unwanted purchases to happen on your account, if you set up the pin currently. It is suggested to have this pin set different to any other pin you own.

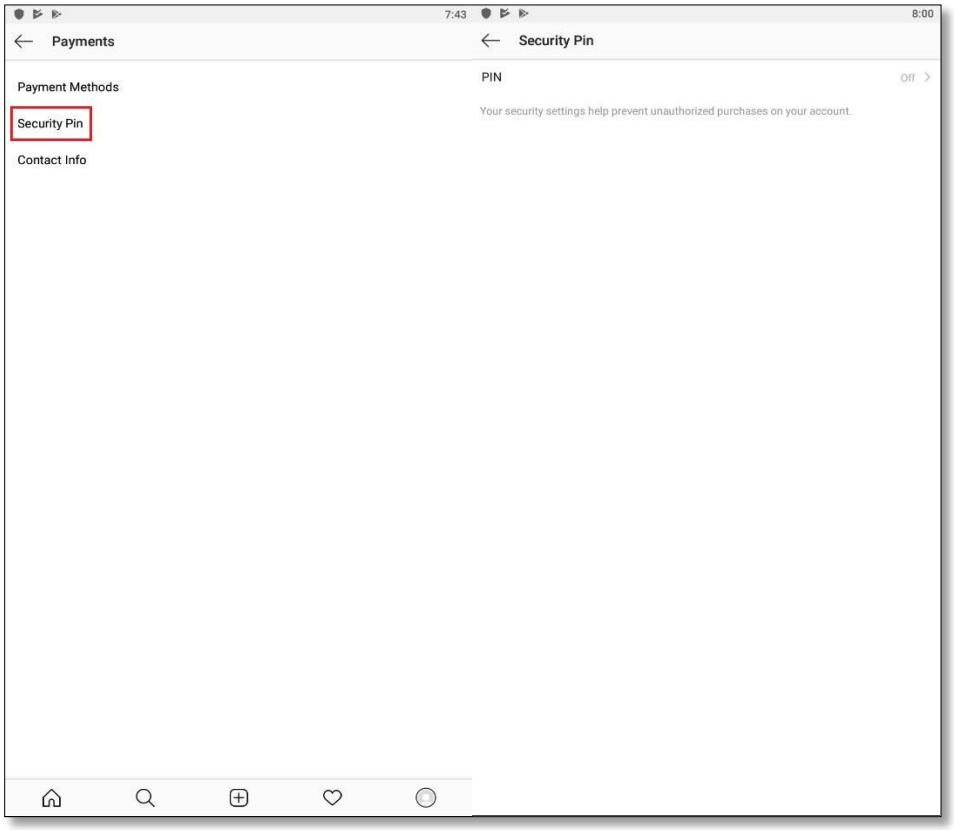


Figure 114 Here we see the option to add a Security Pin to the account to secure the payment option.

You can link your other social media accounts to your Instagram account by going into the Account settings and selecting linking accounts. If this feature is implemented, you can share any content that you post on your Instagram to your other social media pages.

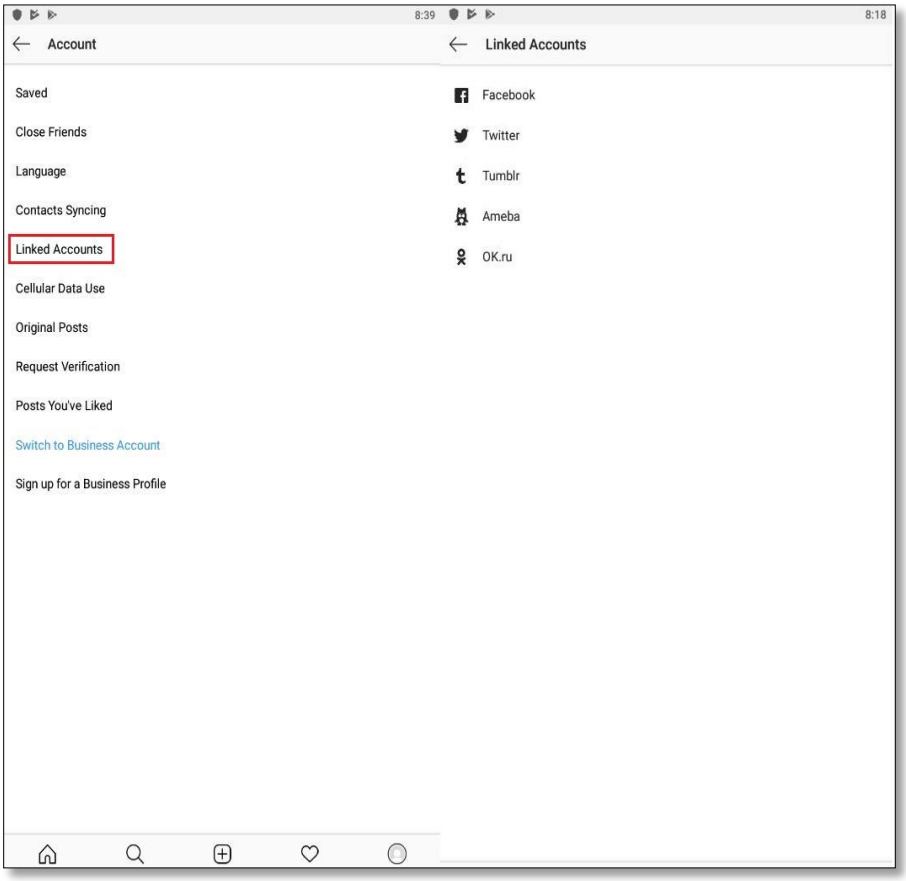


Figure 115 Here we see the option to link an account to your Instagram account

Another option within the accounts option is to sync all your contacts to your account, so any accounts that you have, that their phone number connected to their account will be suggested to you. This is handy if you want to find a friend, however it is not suggested to have if your child is using your phone to access Instagram.

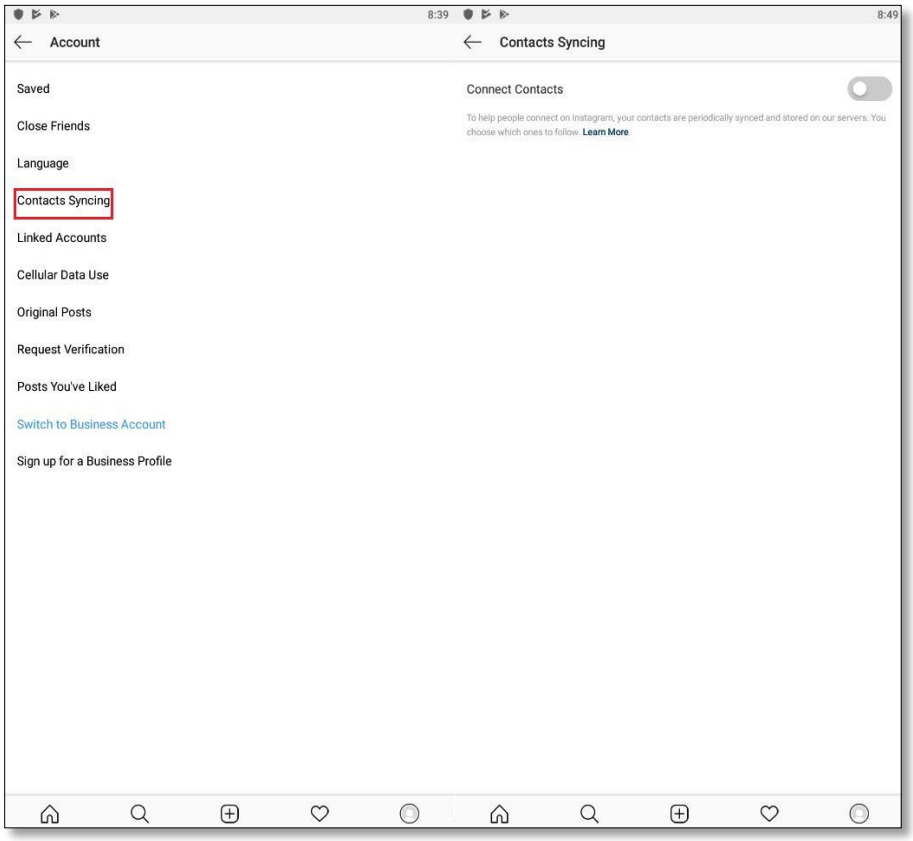


Figure 116 Here we see the toggle to allow syncing of contacts to an account.

When it comes to sharing photos, there is an option to allow the adding of Geo-locations to photos. It is suggested to not use this option at all when posting photos, however if there are already photos that have geolocations posted on them, then they can easily be removed by going into the options on the photo (the three dots) and selecting edit. From here you can select remove the geolocation by selecting the location and pressing the X to remove it.

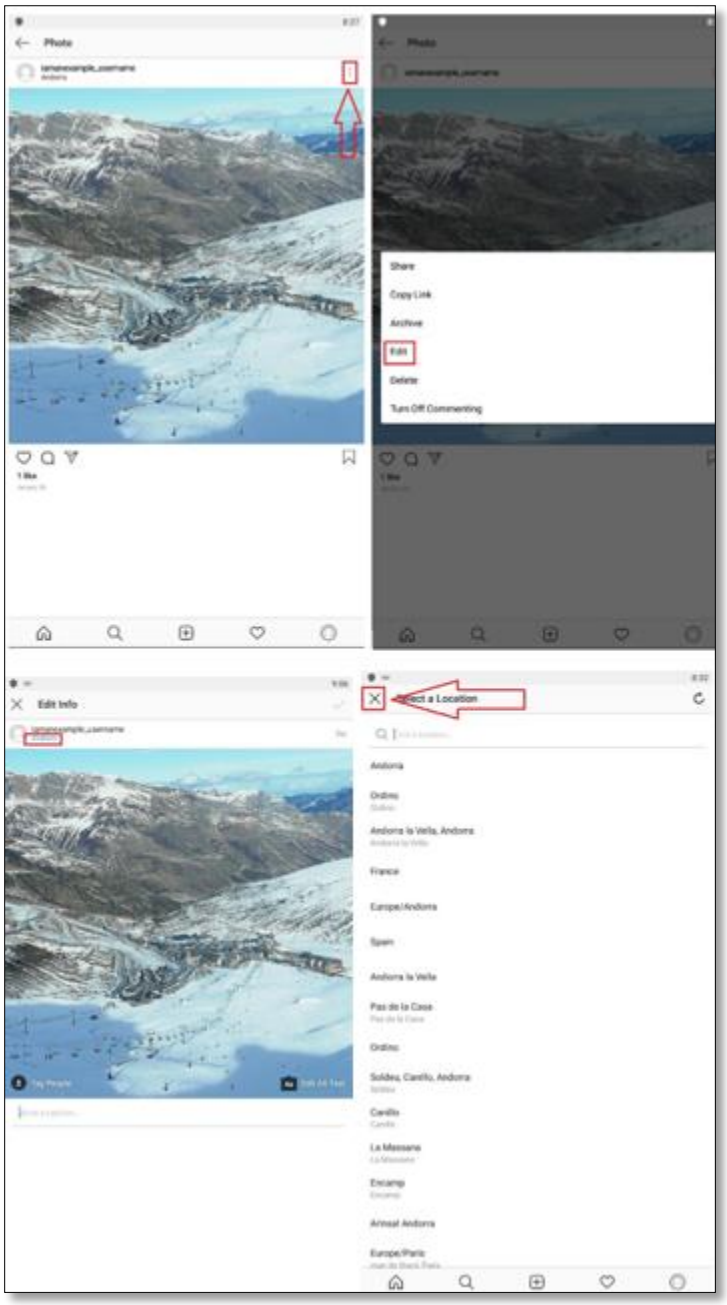


Figure 117 Here we see the process in which a user can add or remove a Geolocation tag.

This will have to be done individually for each photo. It is also suggested to reduce your information on the platform, like phone numbers. This can be done by going to “Edit Profile”. From here you can remove any information connected to the account, like phone numbers, names etc. In this section it is also recommended to set up a pseudonym in place of their own name, as to hide their identity online.

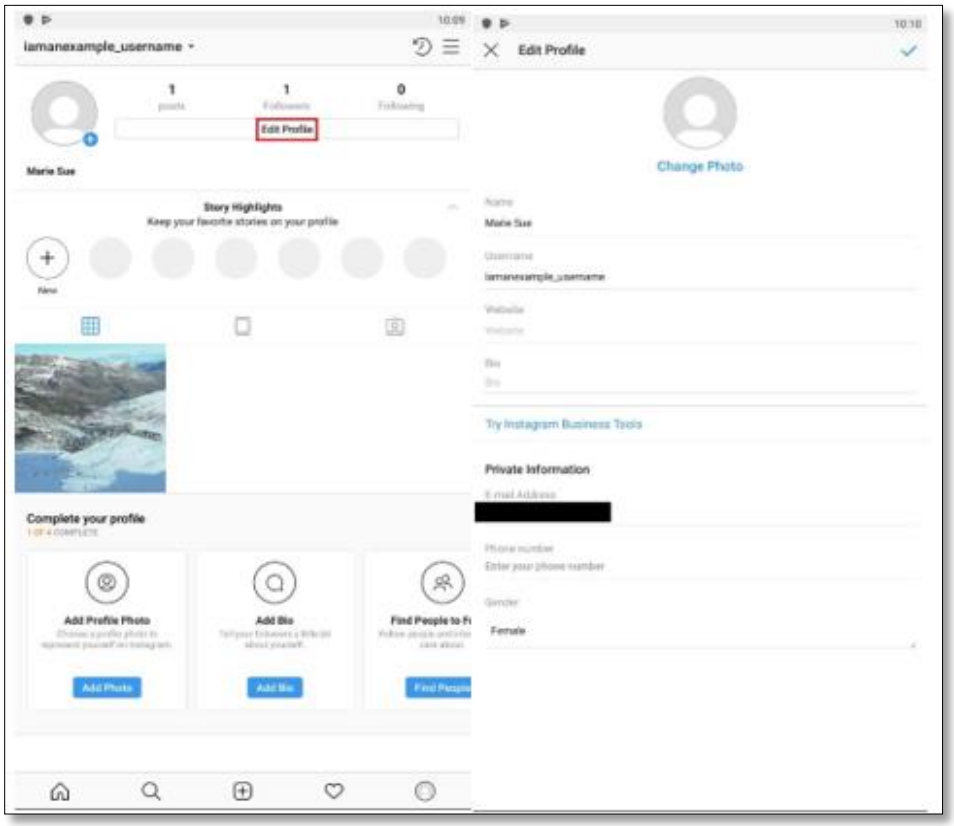


Figure 118 Here we see the options available when editing the user.

Another step in reducing your footprint on Instagram is to remove any tag’s that others have made to your account. This can be done by going onto any photos that they have been tagged in, going to the options on this photo, and selecting the post options. From here you can remove the tag, you will have to do this to every photo that you are tagged in.

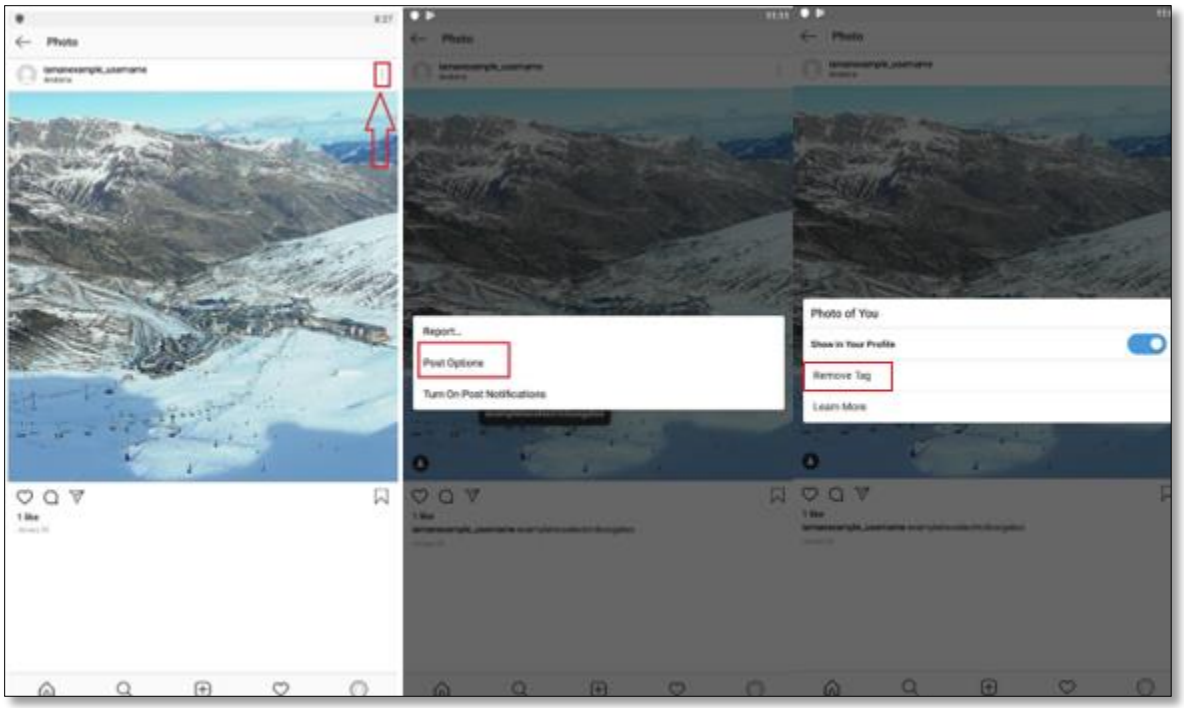


Figure 119 Here we see the process to remove tagging on a photo on another user's photo.

11.2.5 Instagram Best Practice Settings Guide

Having reviewed the settings, we will now offer a best practice guide to the settings we suggest be employed to better protect the child's use of their Apps and their device to increase their safety while accessing online content via Apps:

- Private mode: We recommend setting the account to private mode so that anyone who wishes to see the content your child has posted must request access to it, giving you more control over the viewership. Plus, it allows the user to have anyone who is following to be kicked from following, so if there is an individual who you don't trust, you can remove them.

- Make stories un-sharable: To prevent your child's story being shared around, turn off the ability to share as to prevent such a thing.

- Disable messaging to\ stories: another feature to add on top of stories is disabling people to comment from the stories

- Disable activity status: It is suggested to disable activity logs within settings, as to prevent people from knowing the footsteps of your child on the app.

- Enable offensive filtering: It is highly suggested to enable the filtering offensive comments within the comment controls.

- Enable manual filtering: It is highly recommending enabling manual filtering on comments to heighten the security of the filtering of comments, where Instagram may miss.

- Disable automatic adding of photos to profile: it is recommended to disable the ability for a photo in which your child has been tagged in to automatically appear on the child's account. As to prevent unsuitable content from being attached to the profile.

- Set up two step verification: It is highly recommended in setting up two-step verification in order to protect your account encase anyone else tries to get access to your account.

- Set up a strong password: It is recommended to set a strong password for your account, the suggested amount would be something with over twelve letters, with use of numbers and special characters. This is to prevent your account to be easily accessed by hackers.

- Set up a payment pin: In the scenario that there is a way of payment added to your account, it is suggested to set up a pin that is different than the pin of the card on registered.

11.2.6 Instagram App Safety Rating

Based on our custom App safety rating system and our best practice guide being fully implemented the Instagram App scores as follows.

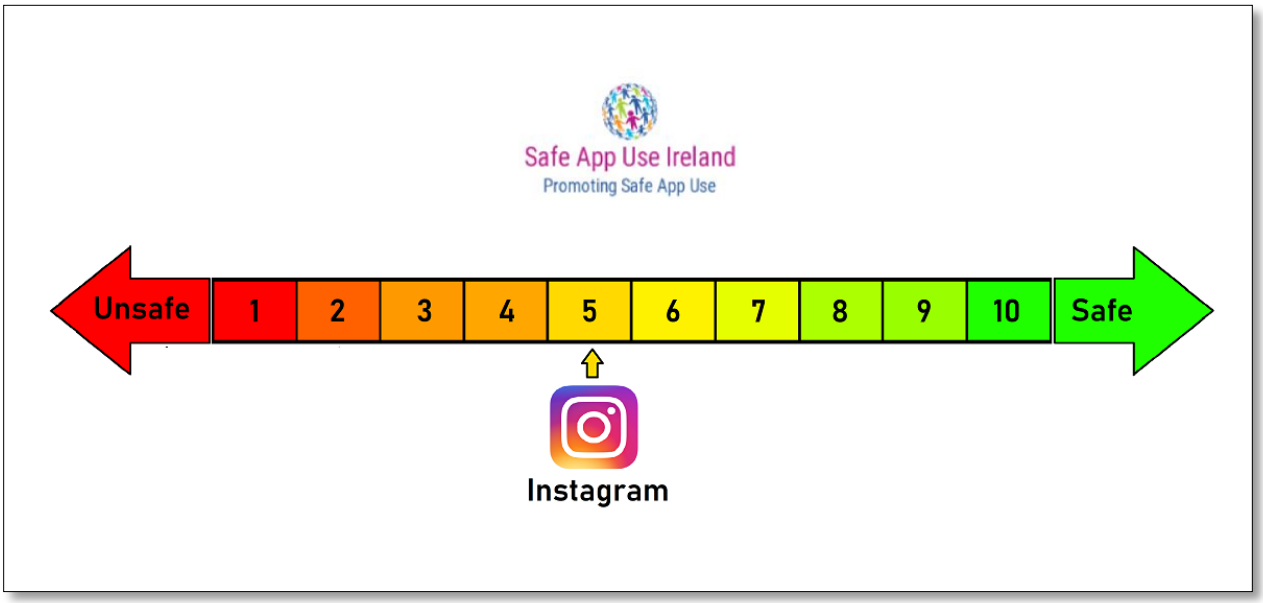


Figure 120 For Breakdown of Points System, please see: 10.0 App Safety Rating System.

11.2.7 Reflections on Instagram

Regrading Instagram, the feature set of Instagram is rather limited, however, the usability is high, and content is easily accessible. While the developers of Instagram have attempted to provide a safe and secure environment, as we have seen, the platform can be easily manipulated. Age inappropriate content is available on the platform.

Data is shared among partners which increases the risk of user data leakage. Most major Apps will share data but once again, we must reiterate this decreases data safety.

The messaging feature coupled with the commenting feature can lead to a toxic atmosphere, so the addition of the ability to block users, refuse messaging connections and delete inappropriate comments does help somewhat to reduce the possibility of this kind of unwanted toxic behaviour.

However, to borrow a common phrase, some things cannot be unseen, so while content can be blocked, it must be seen before it can be blocked, and this cannot be taken back. This is perhaps one of the biggest flaws of this platform. Due to the ease of the availability of potentially age inappropriate content we don't not feel this platform is child friendly. While it is not considered to be a dangerous App, we do strongly consider it to be an App which parents will, should they allow their child to use this platform, wish to strictly monitor.

11.3 WhatsApp

11.3.1 Introduction to WhatsApp.

WhatsApp is a social media App that falls under the Facebook umbrella of products and/or services. It is used as a social messaging App by friends and family to keep in touch. WhatsApp's popularity has surged in recent years raising its profile such that it has become one of the most popular social media Apps on the market today.

It is also one of the most popular Apps in the Irish Market sitting in 2nd place on the Google Android Play Store ranking of free Apps and 3rd on the Apple App Store ranking of free Apps **(SimilarWeb 2019)**. Furthermore, as reported via the RTE article by business editor Will Goodbody **(Goodbury W. 2018, CyberSafeIreland Annual Report 2018)**, 10 Sept 2018, CyberSafeIreland conducted a survey which highlighted that WhatsApp currently retains a following of 33% of the Irish young users, market placing it squarely as the Third most used Platform by children in Ireland.

We conducted our own independent research to determine which Apps where the most popular among Irish children to see if the data supported this conclusion. We asked parents or people with siblings in Ireland to list the Apps their children or siblings preferred. While it seems, there is some debate as to whether YouTube is or is not a social media App, the results do support the conclusions of CyberSafeIreland. If one considers YouTube a social media App, then WhatsApp come in 4th place and if one does not consider YouTube a social media App then WhatsApp claim's the 3rd spot.

Originally designed for the mobile App market, WhatsApp has extended its platform to include the desktop environment on both Windows PC based and IOS Mac devices. This allows for virtually seamless syncing of accounts and facilitates easy switching between communicating via a mobile platform while on the move, and a more flexible comfortable desktop device when sitting in an office or home environment.

Companies also have in recent years begun to adopt WhatsApp as a platform for business use. Usually this is an extension of existing services. For example, many companies will issue order, shipping, delivery status updates via WhatsApp. Some also offer customer support via WhatsApp.

11.3.2 Fees & Charges

There are currently no in App purchases within the WhatsApp platform. There are third-party plugins, such as emote and sticker packages and some of these may incur charges, but these are Google Play Store charges and not WhatsApp charges.

WhatsApp uses mobile phone WIFI and Data, and as such may result in accrued charges via the user's internet service provider or mobile data provider. Again, these are not WhatsApp charges or fees, and users are responsible for managing their own data plans.

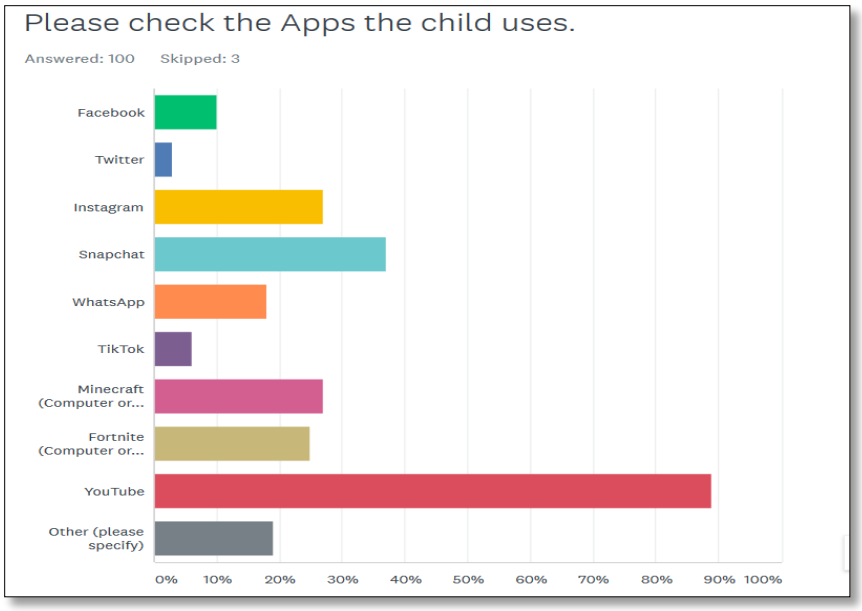


Table 21 Results of Child focused App & Platform use Survey conducted via Survey monkey.

11.3.3 WhatsApp Terms & conditions

Again, we must cover the terms and conditions to highlight the importance of what can be overlooked regarding security and safety if the terms and conditions are ignored. Our aim, once again, is to encourage parents to read the terms and conditions by providing a distilled version which highlights the most important points that may be relevant to a concerned parent.

Your acceptance:

This is your agreement (contract) between you the user & the owners / operators of WhatsApp. This is far more important than people realize as it is the section that states that you agree to all the other stipulations. This section links directly to the privacy policy.

You must register to use WhatsApp's services using up to date correct information including you're your current phone number and should you change your phone number you must notify WhatsApp. You must also agree to provide WhatsApp access to your address book/contacts (in accordance with all applicable laws). You must agree to receive text messages and calls from WhatsApp or third-party affiliates with codes to register for their services.

Ability to Accept Terms & Conditions:

You must be 16 years of age or an emancipated minor or possess, legal parental consent and be fully able and competent to enter the terms & conditions, obligations, affirmations, representations and warranties set forth in the terms of service. WhatsApp is intended for use by those under 16 years of age and those under this age limit are not permitted to use the service. This falls in line with the recent change to the digital age of consent in Ireland which was amended from 13 to 16.

Age Requirement:

WITHIN the European Region you must be 16 years of age or older to use WhatsApp. In such cases where a user is under this age limit a parent or guardian must sign the terms of services agreement on their behalf.

Account Security:

Users must protect their own account by ensuring they use a strong password which is not accessible to unauthorized users.

Privacy policy:

The privacy policy lays out how your data is collected, and shared.

Data Sharing Within the Facebook Umbrella:
Your data is shared among Facebook partners to ensure quality of service, and that features are performing correctly. This also enhances safety and security by removing spam accounts and combatting abusive activity. Data sharing facilitates cross platform, which allows Facebooks platforms to communicate with each other

Nothing is shared automatically between platforms. Only users can share data.

Users should be aware that when communicating with businesses through WhatsApp, data you share with them will be stored on their device/server.

What Data is Collected:

Your Phone number, and all numbers in your phonebook /contacts are accessed. Your email address, if provided may be collected. Profile pictures may be collected. Messages and their contents are not collected or backed up. Once a message is delivered, it is deleted from the WhatsApp servers. Undelivered messages may be stored for up to 30 days on the servers to deliver them, after which; or after 30 days they are deleted. When many people are sharing an item, such as a photo, it may be retained on servers for longer periods of time.

Data may be held for protracted period if there is a good faith belief that such a data may be required to facilitate an investigation.

Device meta-data is collected in all its forms. Location data is only collected if locate related features are used, including sharing your location with other users. This data is collected for diagnostic purposes, not for sharing.

Cookies relating to the WhatsApp website are collected.
Usage and log information is collected. Activity relating to services and service settings, diagnostics and performance fall into this area.

GDPR (General Data Protection Regulations) permit the user to protest the use and collection of Data. You can request access to your information, update information and erase your information via in App settings.

Objections can be raised via this email address: Objection.eu@support.whatsapp.com.
WhatsApp data protection officer for Ireland: DPO-inquiries@support.whatsapp.com.

Privacy Policy Questions can be directed here:
https://www.whatsapp.com/contact/?subject=privacy&eea=1.

Data Protection falls under the Umbrella of both GDPR and the EU-US Privacy Shield Framework.

How is data used:

Measurement & Analytical data is shared with affiliates and businesses to improve services. Personal Data is not shared in this manner.

End-To-End Encryption:
The privacy policy also documents the services use of end to end encryption which promises that only the users at either end of the conversation can read the data. Each message is protected by a unique lock and key system. There is no option to deactivate this encryption. This guarantees that no child will ever accidentally or indeed purposefully deactivate this feature exposing them to increased risk of messages being intercepted.

This also guarantees that WhatsApp themselves cannot view the content of your messages or listen to your calls. End-To-End encryption has been extended to video calling and Status. Encryption is restricted to the user device, not the server, therefore WhatsApp have no facility to decrypt messages. Before a message leaves your device, it is encrypted with a lock with only the intended receiver having the key. Each key is specific to each message.

Terms of Service:

WhatsApp must seek your agreement to its terms to provide services as defined through the its Apps, services, software or website. Registering, installing accessing, using WhatsApp's Apps Services features software or website shall constitute agreement.

Within the European Economic area (EU) or European region, Services are provided by WhatsApp Ireland Limited. All other areas are serviced by WhatsApp incorporated.

Listed under its terms service WhatsApp stipulates that it 'may' provide a safe and convenient way to transfer money. This is a clever way of covering the company from liability should it fail to provide this service, or should the service prove to be unsafe. WhatsApp share connection information with business partners to improve its services. IT is important to remember that End-to-End encryption guarantees that the data within the communication is protected.

Abuse:
WhatsApp aims to continuously monitor any abusive or inappropriate behaviour within its platform. Harmful conduct towards others is strictly prohibited. Automatic systems have been deployed to improve the ability to detect and remove abusive Users that may harm the WhatsApp community.
Abusive users shall be removed.

How users use WhatsApp is analysed to improve all aspect of the service and features.

Data is shared globally among WhatsApp's data centres and systems to ensure global connectivity for its user base. These databases and systems may be operated by WhatsApp OR third-party affiliates which may in turn result in data leakage through data breaches.

Dispute Resolution:

For Irish users local Irish Law Applies to dispute resolution with WhatsApp regarding any issues arising from the WhatsApp terms of service. Irish Courts will be used to mediate dispute resolution.

Termination of Account:

You may delete your account at any time. The deletion of an account is irrevocable. Once an account is deleted it is gone, forever.

Emergency Services Restrictions:

NO access to emergency services is provided through the WhatsApp platform via call, text, video or otherwise. This service is provided by Standard phone or online services only. These service access restrictions include fire, medical, law enforcement. Coast guard or any other emergency services no stated.

Acceptable Use of Services:

Services must be used in accordance with terms of service. Abuse of the terms of service may lead to a user being banned. If this happens, a banned user is not allowed to create a new account. So if a user who is abusing your child is banned, and creates another account to continue harassing your child, this account is also subject to banning.

You must use services only for legal Authorized and acceptable purposes. Assisting other in violations is considered a violation. Furthermore, any acts that are illegal, obscene, defamatory, threatening, intimidating, harassing, hateful racially or ethnically offensive, or instigate or encourage conduct that would be illegal or otherwise inappropriate are prohibited. Promoting violent crimes, or involve publishing falsehoods, misrepresentations or misleading statements, impersonating somebody, sending illegal or impermissible communications such as bulk or spam messaging; auto-messaging or auto dialling is also prohibited. Services are for personal use only unless authorized by WhatsApp. This section highlights that activities such as the widely publicized MOMO incidents would automatically lead to a ban for all users sharing such content.

User License to WhatsApp:

As a user you grant license to WhatsApp to operate and provide services to you. You also grant worldwide non-exclusive, royalty-free, sublicensable rights for WhatsApp and transferable license to use, reproduce, distribute, create derivative works of, display and perform the information including content you upload submit, store, send or receive on or through our services. This is important in that end-to-end encryption should prevent WhatsApp having access to your data, however, if your data becomes viewable and/or useable, WhatsApp will have rights to it. Keep this in mind.

Access to your personal Data:

You must allow WhatsApp to access contacts, however this data is not collected as it is Third-party data and not yours to offer up.

Unauthorized use of your Phone:
You must notify WhatsApp immediately if any unauthorized person uses your device and you are personally solely responsible for any status updates posted from your device.

Collection of Personal Data Statement:

Users must not attempt to collect other user's personal data such as phone numbers.

Spam/Solicitation:

Spamming or solicitation for commercial purposes is prohibited.

Visibility of what you share with other user's:

The content you upload shall only be viewable by those to whom you grant access, by allowing them to have your contact details stored in their device and adding you as a friend. A blocked user shall be denied further access to your content.

Status update and Content Posting Responsibility:

The user is solely responsible for any content they post and accepts that they will be exposed to content they may deem inappropriate even should it violate the terms and conditions. In such case WhatsApp may need time to remove the offending content.

Warranty Disclaimer / limitation of liability:

You acknowledge that you assume all risk involved with using the service and the WhatsApp company shall not be held responsible for any incidents that occur on the platform.

Inappropriate Status updates:

All content you, or others post must conform to the terms of service.

Impersonation:
Yu are not allowed to impersonate other users.

Adult Content:

Adult content must be clearly identified as such.

All the above content has been thoroughly filtered and distilled. It should not eb considered legally binding. The full terms of service can be found here **(WhatsApp 2019)** as well as the privacy policy **(WhatsApp 2019)** and the data sharing policy **(WhatsApp 2019)**.

11.3.4 WhatsApp Features

WhatsApp is primarily a text messaging App which allows people to send text messages via their internet connection. These text messages are free of charge from WhatsApp. Charges only via the user's internet service provider or phone service provider, if for example the user exceeds their allotted data plan. It is the user's responsibility to monitor this.

WhatsApp has extended its functionality to include video calls. As such it has access to your phones camera and can take pictures to add to chats. You may also use your phones gallery to add previously taken pictures or downloaded content to chats. In addition to being able to send pictures, users may also send Documents including PDF's, spreadsheets, slideshows and so on, up a healthy size restriction of 100mb. This allows users to share reasonably sized documents without the need to switch to E-mail Apps. The size of file sharing that WhatsApp's offers is quite good compared to other similar Apps, such as Discord, a recent rival to WhatsApp whose user based is steadily increasing, but who's file sharing size is limited to 8mb on a free account and 50mb on a subscription to their upgraded account service, Nitro.

WhatsApp allows for group chats to be created and managed, allowing up to 256 people per chat to conversate and share information, pictures, videos, and sound files. Chats can be customized allowing the name of the group to be changed and chat profile picture to be changed. You may also mute a chat. Chat options further provide the ability to report, block, mute, clear, and export a chat. A shortcut to a chat can also be created which places the short cut directly on your device's desktop environment.

WhatsApp has many interesting security and quality of life features and settings which will be covered in depth in another section of this report, for example, if you select and hold a message in a chat, you can unsend the message deleting it not only from your own device but from the entire conversation. This is a very useful feature in situations where a mischievous child might send an unauthorized message, or a parent finds their child has sent in appropriate content or revealing data via a message. This is not a guarantee that the data has not been otherwise saved on the end user devices, but it is a worthwhile security feature none the less and one that frankly we feel all such messaging Apps should adopt.

11.3.5 Money Transfer via WhatsApp Payment

WhatsApp money transfer is a beta program currently being tested in countries such as India. It is currently (as of 26th Jan 2019) not available in Ireland, however, it is designed to facilitate the payment of bills and the sending of money between WhatsApp users by implementing the UPI (Unified Payments Interface) which requires activation, as discussed by correspondent Aatif Sulleyman **(Sulleyman A., 8th February 2018)**, article for Independent.co.uk online. Once the UPI has been implemented, the user can then link in their bank account, and send money via a 'Payments' option in the user settings.

While is not beyond the bounds of possibility that a child may figure how to implement the UPI and select the payments option, the risks associated with unauthorized payments is far less significant than it is in other similar Apps or video games.

11.3.6 How Safe is WhatsApp?

WhatsApp uses 60-character End-to-End device-based encryption. This means that a private key code is generated between two users, which is stored only on each user's local device. The corresponding public key must be used if the message is to be read. Encryption is not perfect in any case, but encryption does afford a reasonable level of peace of mind and security.

To crack the encryption a 'hacker' would require a huge amount of computing power and a long period of time. It might be possible for a mis-user to guess an encryption key, but the odds of this happening are extremely low. This means that the only reasonable fast way to access a chat a mis-user should not have access too, is to gain access to a key, which means they would have access to the device allowing them to view the conversation or data in plain text.

What does all of this mean to the end user? Well, it means that your data's safety can be rated as very high. As these encryption keys are stored on the end user devices and not on WhatsApp servers, not even WhatsApp can view the data contained within a chat.

11.3.6 Shared Data

Data shared via chats, is deleted immediately upon delivery, from the WhatsApp servers. In cases where delivery failed, data is normally kept (encrypted) for 30 days to facilitate further attempts to deliver the data/message.

In extreme cases data may be held longer, for example; in cases where there is a good faith belief that the data may be needed in an account investigation. Or in cases where a legal request for access to account data / chat data has been made by legal or law enforcement authorities. However, users should always remember, your data is only as safe as the user with whom you are sharing your data. A person with whom you share data is free to share that data on with whom-ever they so choose, so users must think very carefully about who you, or they, add to friends, contacts list, phone books and what data they share.

Data shared with companies is retained on the companies end user device, and as such the data protections of WhatsApp will no longer apply. Users again, should think very carefully about what they share with companies and investigate the data retention, sharing and deletion policies of any companies with whom they are considering sharing data.

11.3.7 WhatsApp & Facebook Family Data Breaches

How secure is the data you share via WhatsApp? Are your private conversations private? Are large Scale data breaches leaking your details? These are more and more common questions as data breaches with large companies become more and more prevalent. Where once user's may have been almost nonchalant with their data, they are now becoming increasingly awakened to the widespread leaking and the dangers of data leaks.

As we examine the history of data breaches pertaining to the WhatsApp platform we find that there are instances of what might be termed 0day exploits. This is fairly common practice in the software development world. It occurs when a flaw is discovered in a programs code and is exploited allowing access to features otherwise restricted or manipulation of code to force it function in an otherwise unforeseen manner.

The most serious of these, as discussed by Wakabayashi D., 2018 in the New York times article **(Wakabayashi D., 2018),** occurred when a cyber security company discovered a vulnerability which allowed users to alter the 'Quote' function of the application, which allows users to quote previously posted messages. This did not allow potential scammers to access user's data directly, but it did facilitate the spreading of disinformation through the platform. This Flaw has now been patched.

There are also some security concerns surrounding third party affiliates as discussed by a staff writer at Business Tech News, 22nd Sept 2018 **(Staff Writer 2018)**. This is related to WhatsApp partnering up with services such as Google Drive which facilitate the backing up of chats and user data outside of WhatsApp's own servers (remember under ordinary operating procedure data is deleted after 30 days if undelivered and deleted immediately if delivered). Google Drives security protocols have come under scrutiny recently with several breaches particularly in the South African data centers.

The greatest concern however, which should surprise nobody; is the risk of data leakage through Facebooks lacking internal security, and eagerness to monetize user data. WhatsApp data is shared universally through the Facebook platform. The recent Facebook data breaches, leaking of sales agreements between Facebook and its third-party partners which could potentially give access to user's private messages is of huge concern. Not to mention, the now infamous scandal surrounding Cambridge Analytica has resulted in hefty fines in many countries, congressional hearings in the United States, the rushing of GDPR in the European union and a severe almost unbelievable loss of trust, and market share for Facebook. The scale of these incidents is simply massive in scope and far beyond the scope of this research project. However, should readers want more information, information may be found here documented by The Guardian's online website **(Guardian editors, et al 2018)**.

The Facebook parent company has made efforts to increase its security, transparency and data privacy practices, but trust is still very shaky. However, of all its messaging platforms, WhatsApp is perhaps the most secure, and the proper application of security settings can greatly restrict the data that is available to be shared and thus the risks.

11.3.8 WhatsApp's Personal Security Optimization Options

Here are the Security features available for WhatsApp

- Manage account visibility
- Manage GPRS location settings
- Manage Users (Block, Report)
- Manage account security (Two step verification)
- Manage chat settings (backups, Delete Chats)

In the section below, we will go into detail on how these actions can be performed.

11.3.9 WhatsApp Settings

General App Setting:

Users select the general App settings by select the three dots at the top right (which denotes a settings menu) of the screen as seen below.

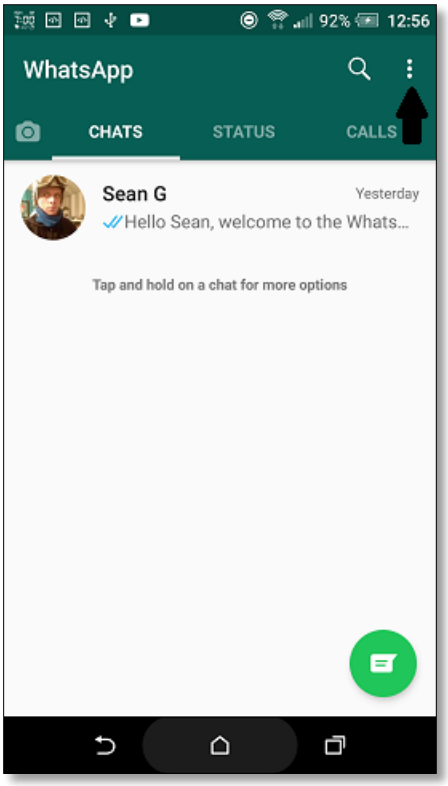


Figure 121 Select the three dots to enter settings menu.

Next, select settings from the available options. This will enter the settings menu.

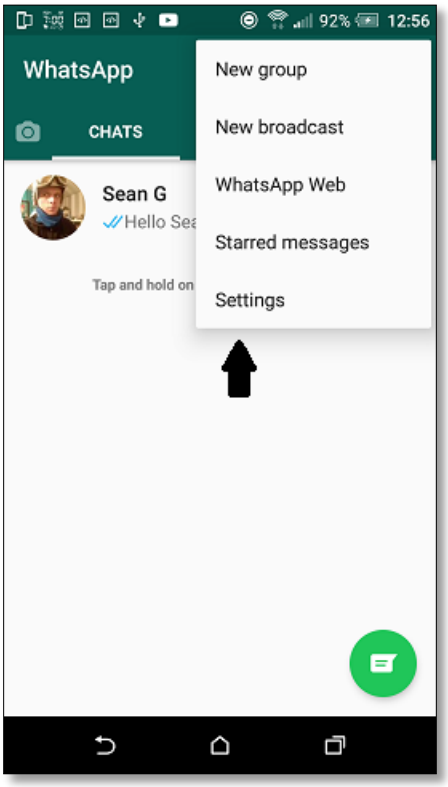


Figure 122 Now Select settings.

You will now be in the main settings menu from which we will begin to adjust App settings to restrict the sharing of user data.

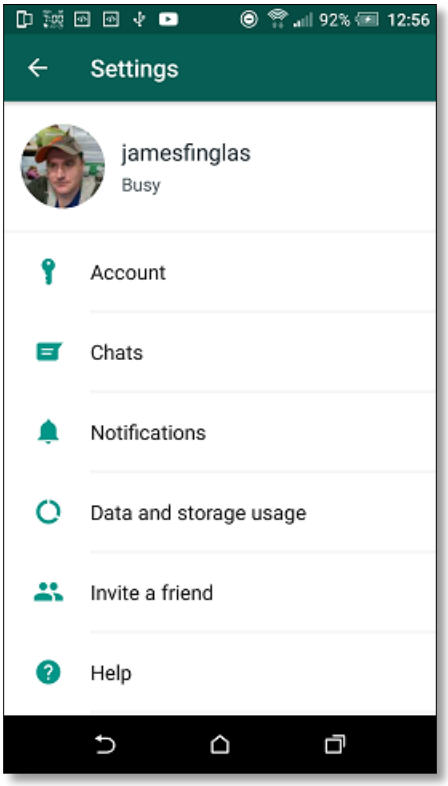


Figure 123 Here we are at the main settings menu.

Accounts:

Privacy:

This menu is important from the perspective of parents who wish to reduce the online footprint and visibility of themselves or their child while using the WhatsApp platform.

Last Seen / Profile Photo / About:

These settings are all very similar in nature. We recommend that Last seen status is blocked from all users, profile photo be restricted to contacts and the about status be restricted from all user. This will help to restrict the user's online footprint.

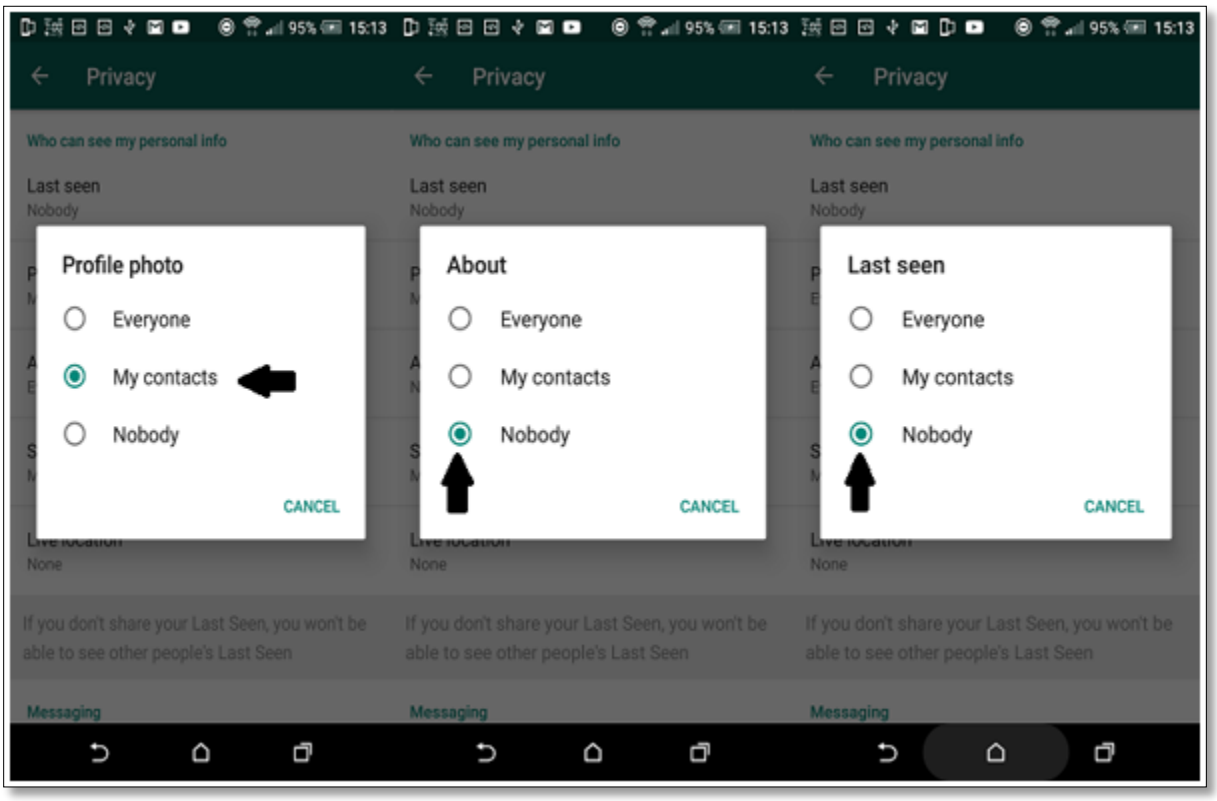


Figure 124 Here we see the 'Last Seen', 'Profile Picture and 'About' settings options adjusted to reduce online footprint.

Status:

Status displays whether a user is currently available, away or busy. This setting might be seen as fairly innocuous however for peace of mind we recommend that either the option to include contacts individually or exclude contacts individually be used. This will restrict your status updates to only those you specifically wish to share them with or restrict those you specifically do not wish to share them with.

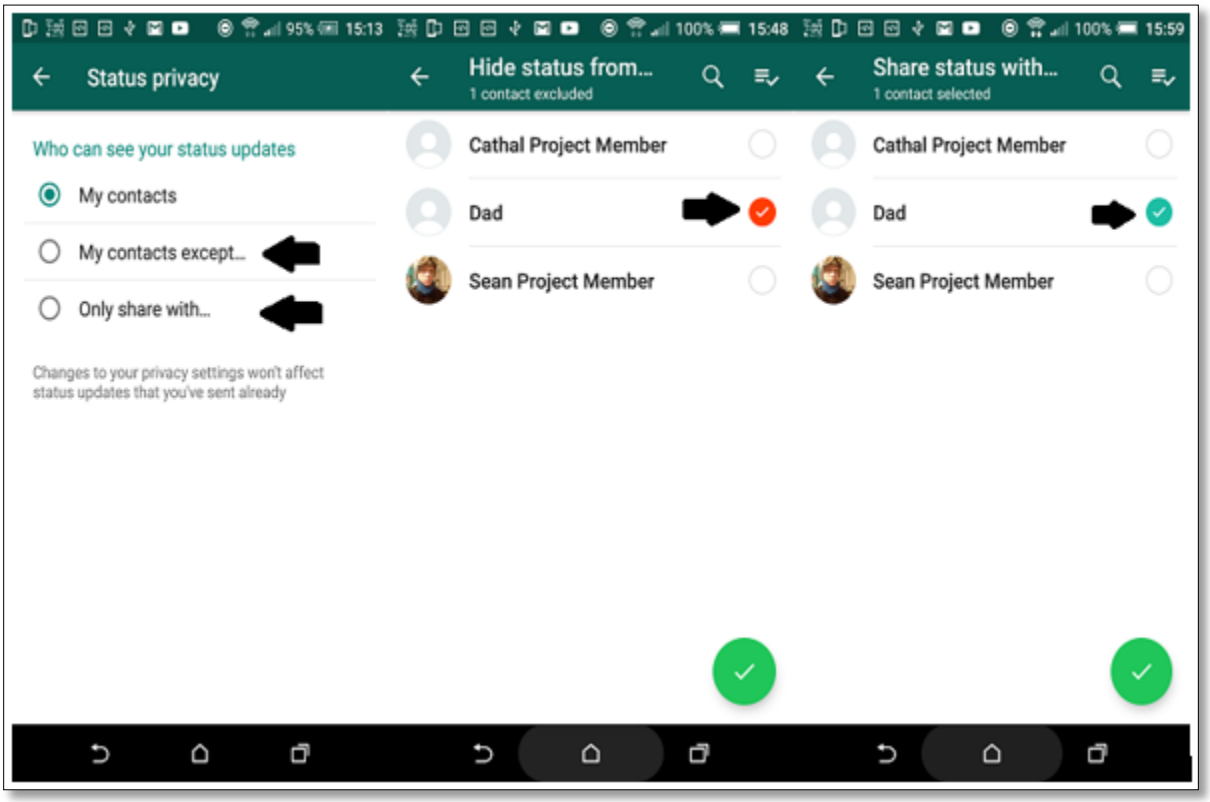


Figure 125 Here we see the status sharing options displayed, with sharing to all excluding one contact shown first, followed by sharing restricted to one contact. First, 'Dad; is restricted from seeing the status, then status is only shown to 'Dad'.

Live Location:

This setting controls the ability for WhatsApp to display and share location sensitive data. While you there are no options to here, the options are controlled by device settings. If you turn off GPRS based location services on your device, this data is no longer accessible via WhatsApp. An immensely important security feature where children are concerned.

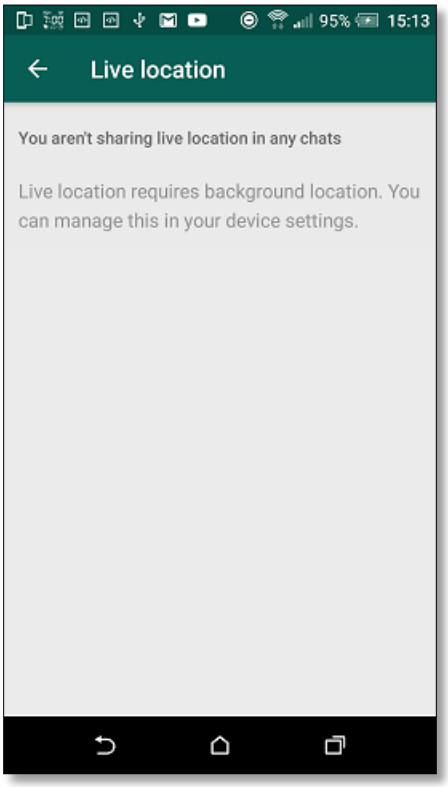


Figure 126 As seen above, GPRS based location services are deactivated on my android device, therefore WhatsApp cannot collect or display location-based data.

Contact Blocking / Deleting:

Contact blocking in a simply process involving selecting the option from within the privacy settings, then selecting the contact to be blocked. This will add the contact to a blocked list contained here.

The process of unblocking a contact is done from the same menu.

As a further measure, should a parent wish to permanently block a contact from contacting their child, the individuals number can be removed from the device contact list. This will not just block the contact but preclude that contact from ever contacting the child again through WhatsApp.

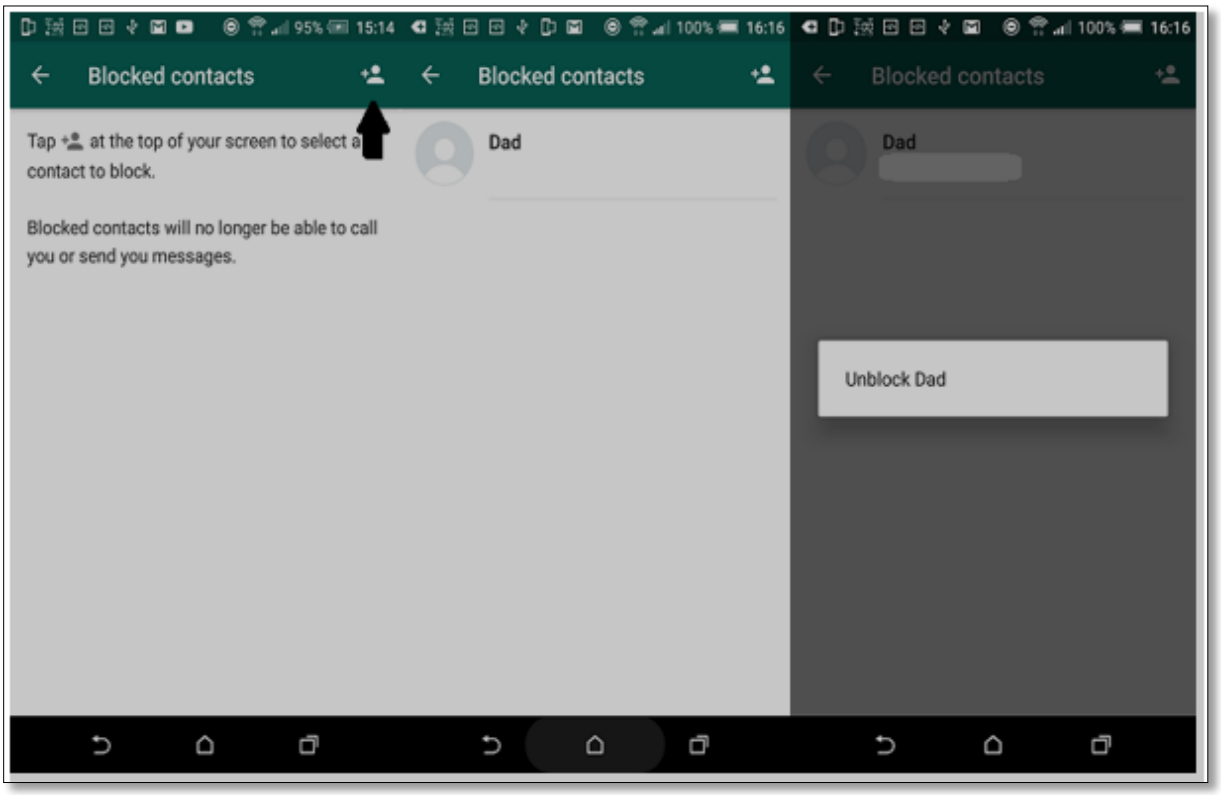


Figure 127 Here we see the contact blocking options.

Read Recipients:
This options simply allows a user to tell if a message has been read by the recipient. This does not involve any data sharing. It is a simple toggle option. We do not see any security risks associated with this option.

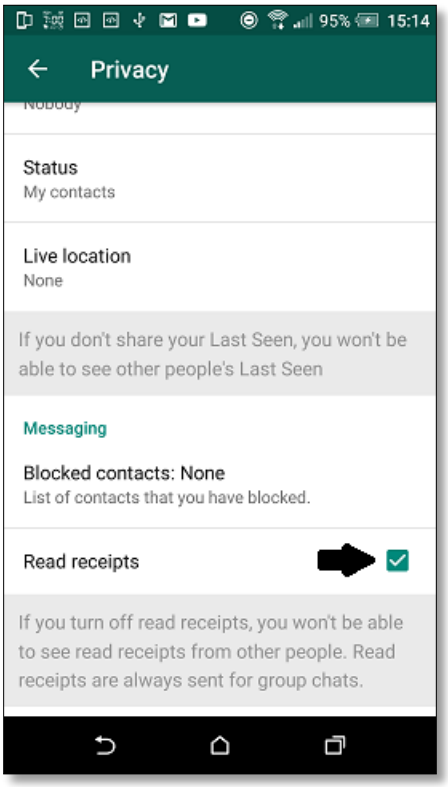


Figure 128 Here we see the toggle option for 'Read Recipients'.

Security:

Returning to the main account settings menu we next select security. In here we set turn on security notifications.

With End-to-End encryption, encryption keys are stored on the devices of senders and recipients. These keys will not change under normal circumstances. However, in rare cases they might. For example, should a user change phone number, and use the proper procedure to change number their encryption key will change as their account has changed. Your chat is still encrypted, and the Encryption keys will resync the moment a message is sent.

User's will be notified that a key has changed, enabling them to contact the user and verify that it is them and that the keys have resynced, just in case the encryption has somehow been broken, which is extremely unlike, but not impossible.

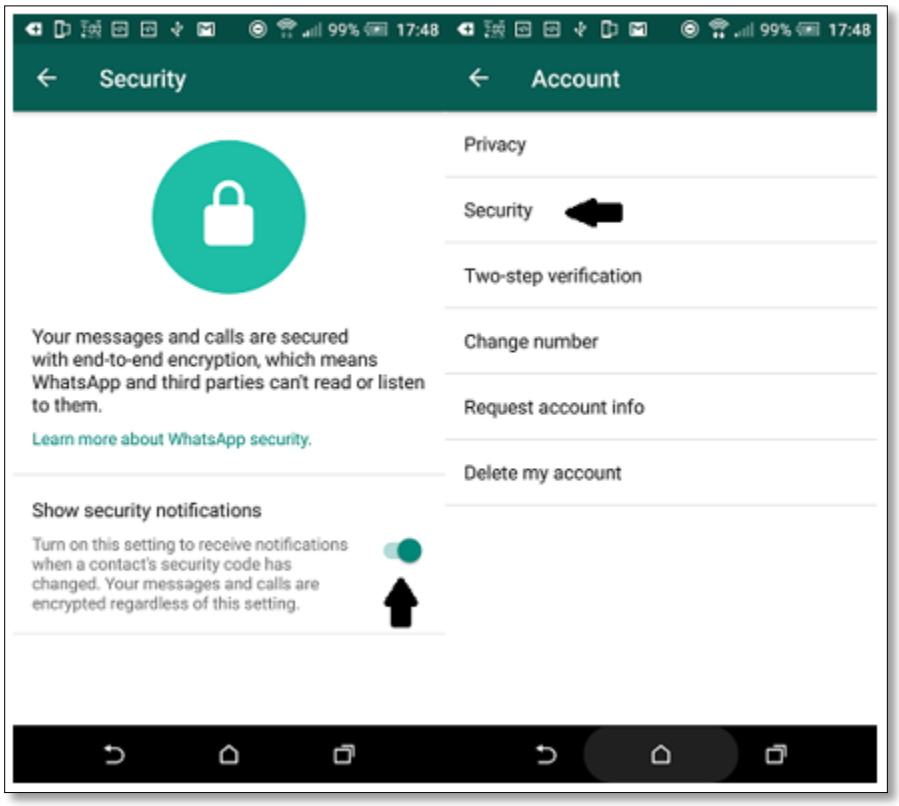


Figure 129 Here we see the security options selected and security notifications enabled.

Two-Step Verification:
Two step verification is account security setting with aims to make it more difficult for unauthorized users to download and access your WhatsApp account. This locks your phone number to a pin number.

Returning to the main account settings menu we select Two Step Verification from the menu. We are then prompted to enter and reconfirm a pin number. Next, we are asked to enter and reconfirm an E-mail address which we will use should we forget our pin number to reset. Finally, we will see a confirmation message confirm we have set up Two Step Verification. Should we wish to reset Our pin, or E-mail, we simply renter the Two Step Verification menu and are offered prompts to do so as seen below.

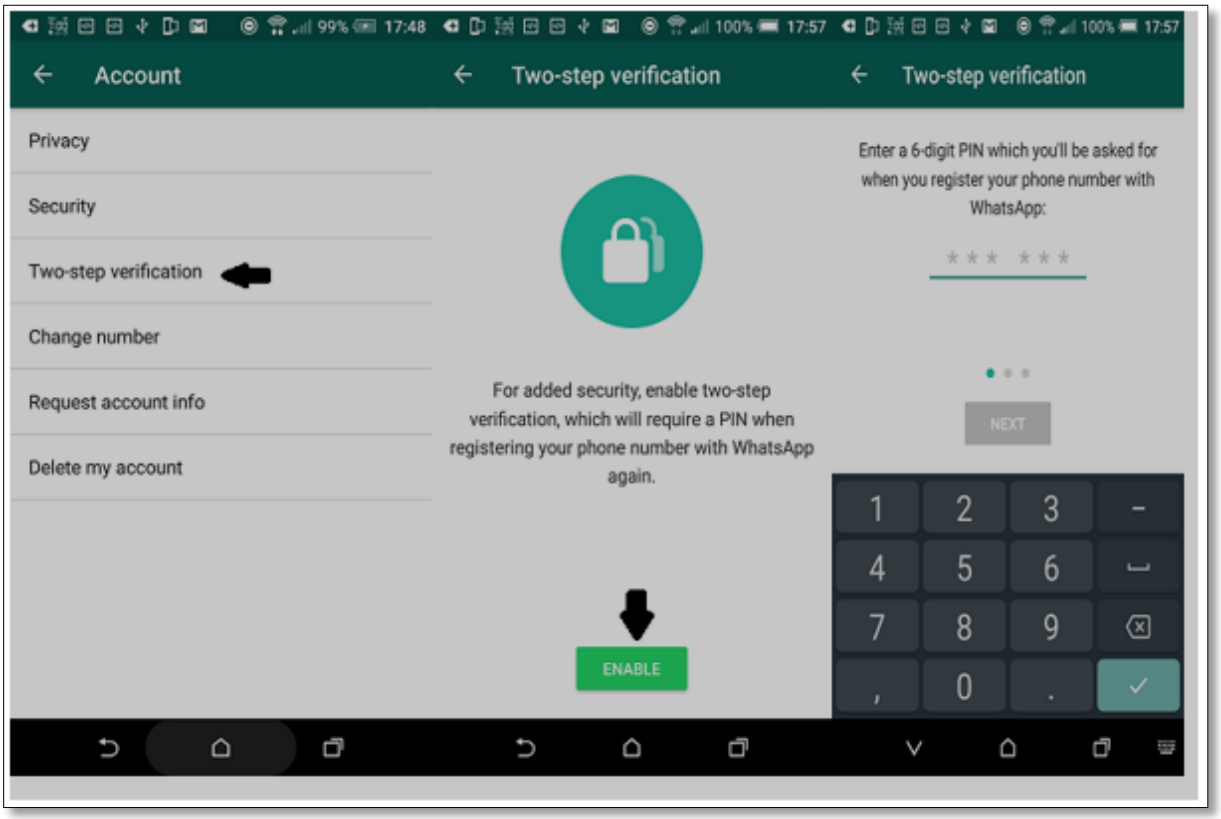


Figure 130 Here we see the setting up of Two Step Verification. First, we select the option via the main account settings menu. Next, we select enable. We are then asked to enter and reconfirm our pin number.

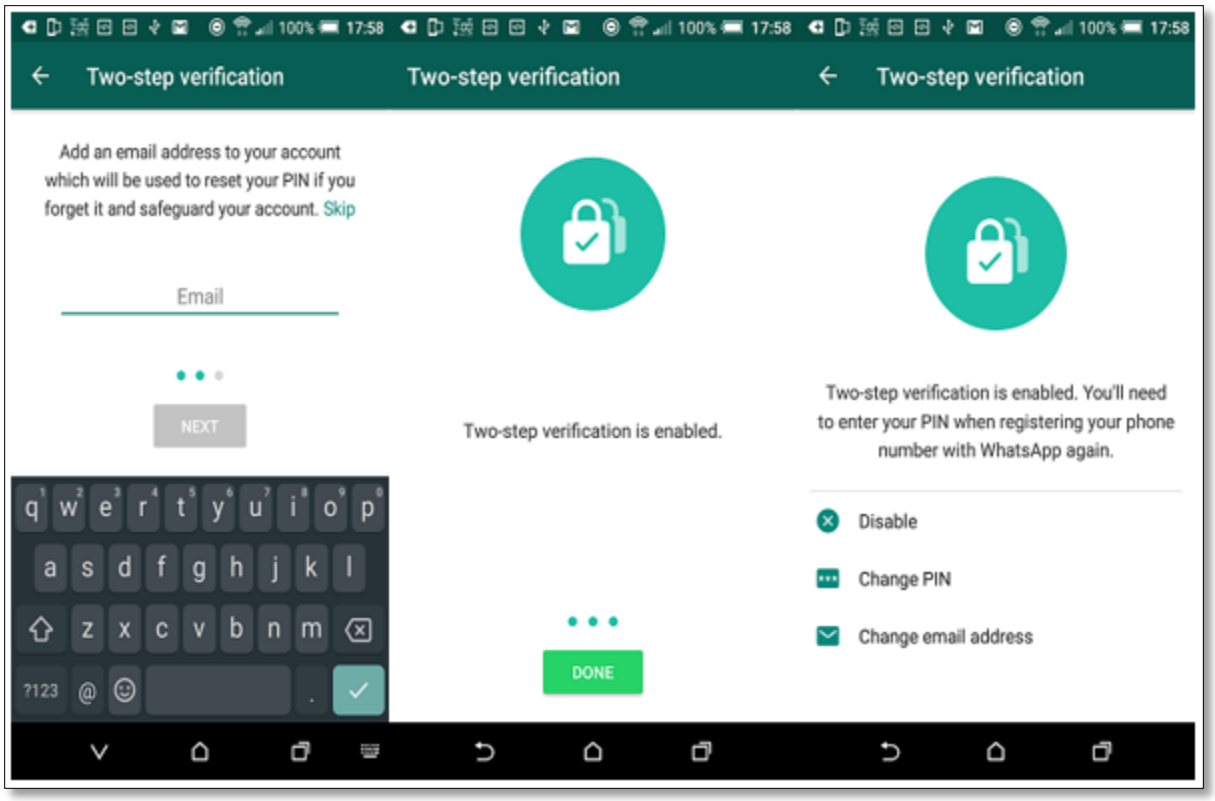


Figure 131 Finally, we enter and reconfirm an E-mail for resetting our pin, and we receive a setup confirmation message. Should we wish to reset any details we simply renter the Two Step Verification menu.

Request Account information:

Users may request their data from WhatsApp. Requests take up to three days. Requesting one's data is a useful way to confirm if your data is being restricted. For example, prior to enabling these settings as we suggest, a user might request their data, then adjust the settings; finally requesting their data again and doing a direct comparison.

To request Account Information simply return to the main account settings menu and select the 'Request Data' option. On the next screen, simply select the option to request your data. You will be presented with a message stating that your data will take approximately 3 days to download and will need to be downloaded once available, as seen below.

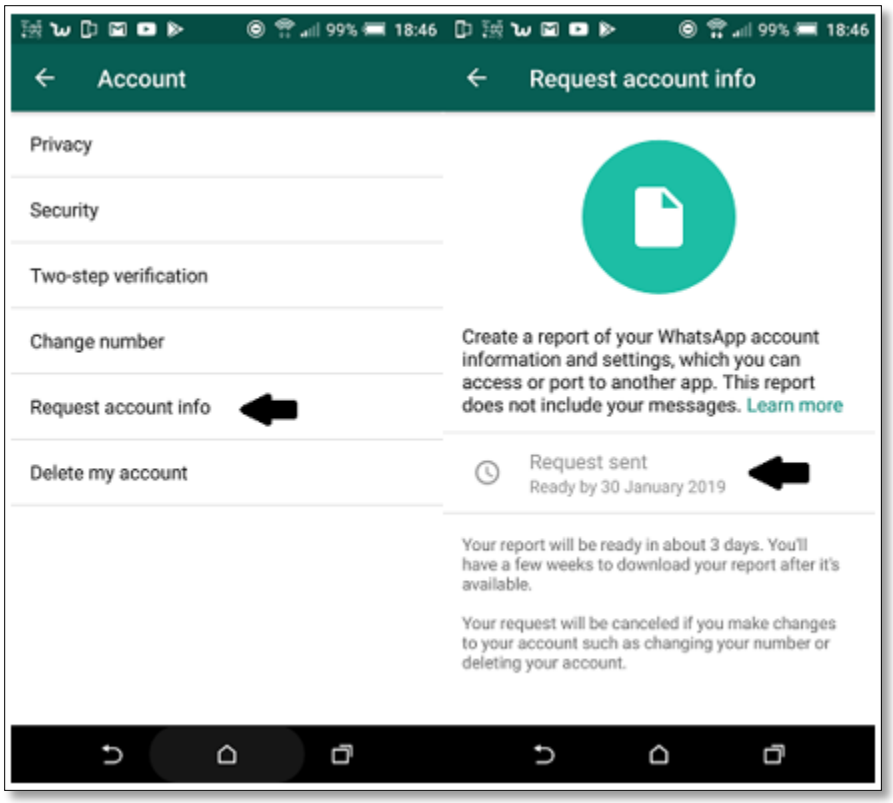


Figure 132 Here we see the Request Account Info option highlighted.

Chat Backups:

As mentioned previously, chat Backups allow you to export a chat to a third party. This can be done individually at any time from within a chat as seen below.

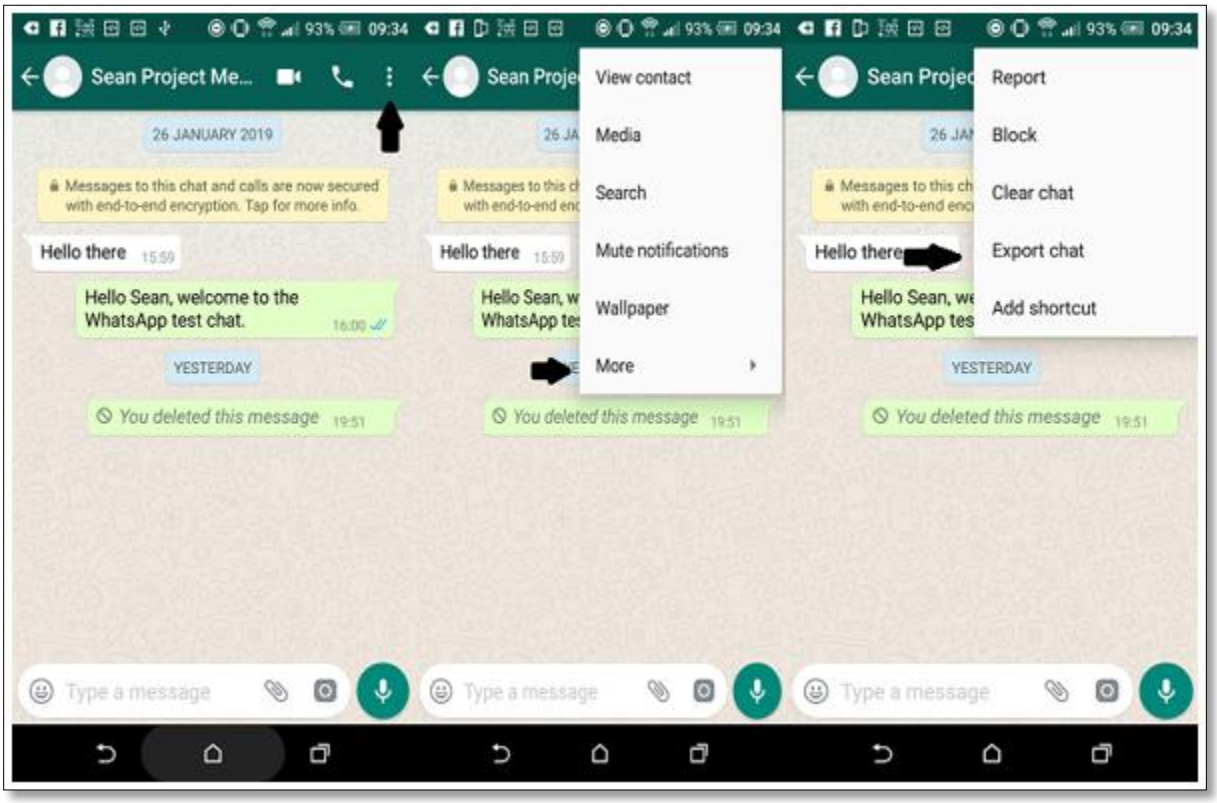


Figure 133 Here we see the in chat 'Export Chat' options highlighted.

However, chats may also be set to backup automatically, or at pre-determined times, or disabled entirely. As previously mentioned, backing up chats to a third-party carries an inherent risk of data leakage. We recommend that automatic backups be disabled. Chats may still be backed up individually as and when needed. However, if security is the main concern, chat backups should be avoided. Furthermore, users should remember; when backing up data to a third-party service you enter that third-parties' terms & conditions and depending on the third party your data may be shared.

To disabled automatic or scheduled chat backups, return to the main user settings. Next, select Chats setting. Next, select ‘Google Drive Settings’ and set the chat backups frequency to ‘Never’ as seen below.

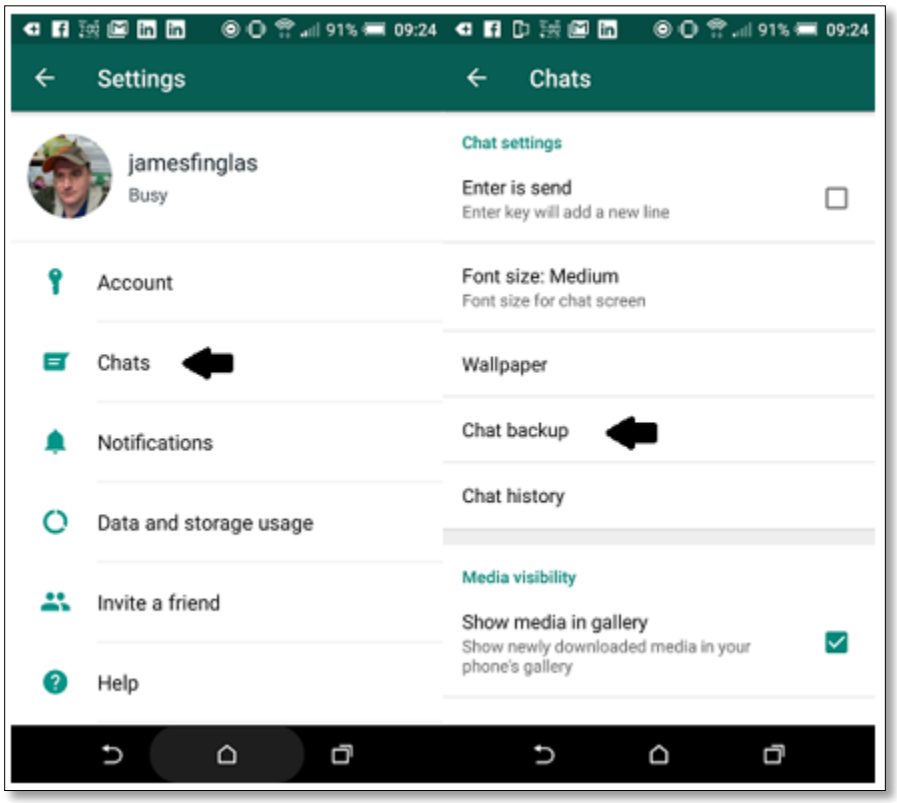


Figure 134 Here we see the chat settings being select from the main settings menu, followed by the chat backup option being selected.

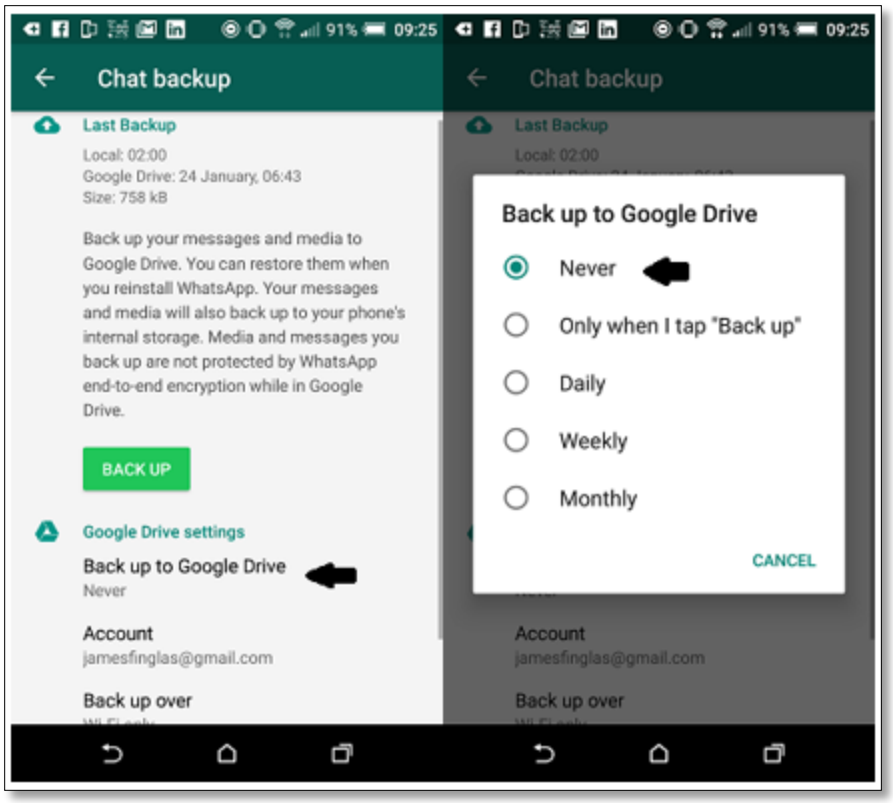


Figure 135 Here we see the 'Google Drive' settings being selected, and the chat backup frequency being set to 'Never'.

Delete Chat Content as needed:

As mentioned previously, users can delete content as needed from chats. A user may delete any content they have sent from either their local device, or from all devices linked to the chat. Users also may delete any content the find inappropriate or offensive from a chat which another use has sent, however; this will only delete the offending message or content from their local device, not the entire chat.

To delete content, simply highlight the desired content. Tap to select this content. Tap the delete icon from the top of the chat, then select the desired deletion method. The content will then be deleted from the local device, or the entire chat depending on the chosen option. As seen below.

DISCLAIMER* This will not delete any local backups of the content which have been saved to other locations, on any of the devices belonging to users connected to the chat. *Disclaimer

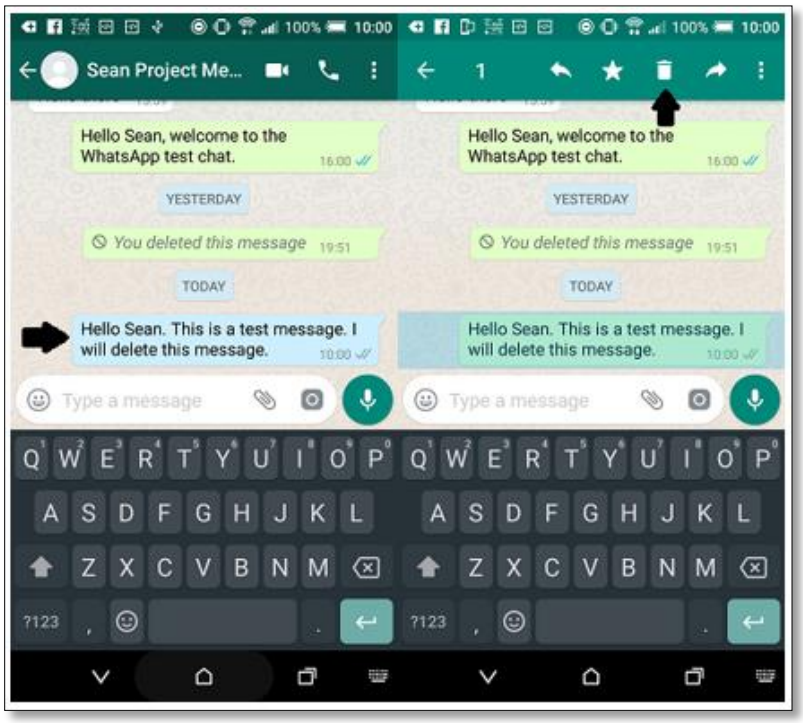


Figure 136 Here we have selected the content we intend to delete, by tapping the desired content. Next, we select the delete icon from the top of the chat.

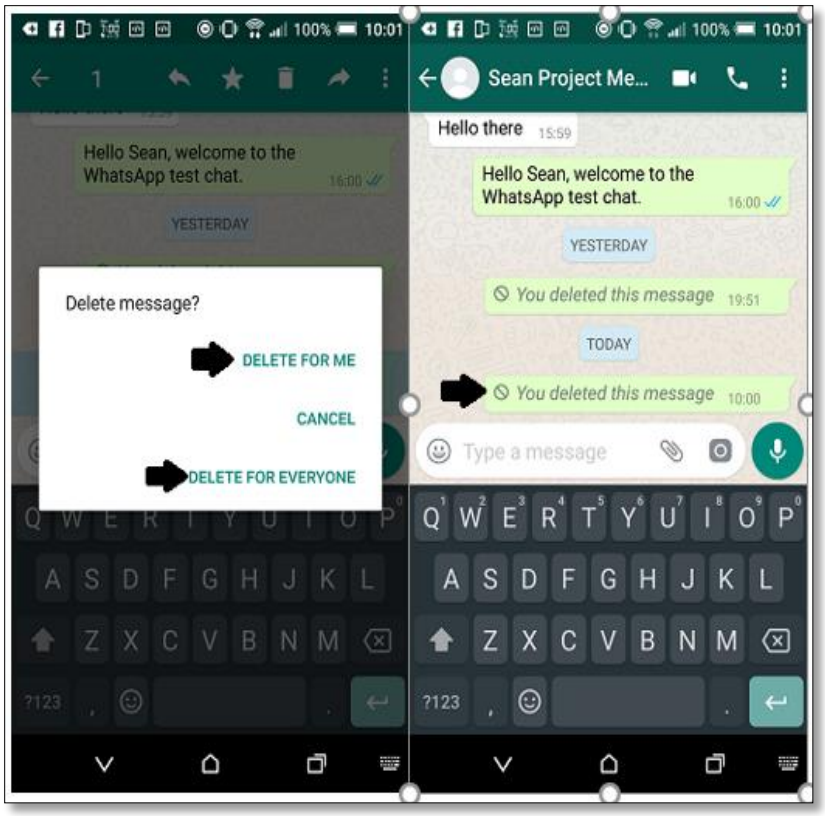


Figure 137 Here we see the available options for deleting the content from within a chat.

Report a Chat:

Should a parent, or child find themselves the victim of an abusive user, or offending content leading to them wanting to report a chat, a feature is provided to handle this from directly within the App. This feature also allows the user to block the user and delete all content automatically as part of the reporting process.

To report a chat, simply select the chat option via the 3 dots on the upper right of the chat window, then select more. Next, select report, leaving the 'Block this contact and delete this chats messages' option pre-selected should you desire.

Remember, should you wish to report this user further and lodge a dispute against the user using the report abuse function on the WhatsApp website, you may wish to keep any relevant data from within the offending users chat

Finally, select 'report chat' and the chat report will be sent for review by WhatsApp as seen below. Please note, due to data protection laws, and GDPR laws, you may not see any outcome from this, but this does not mean WhatsApp have not investigated.

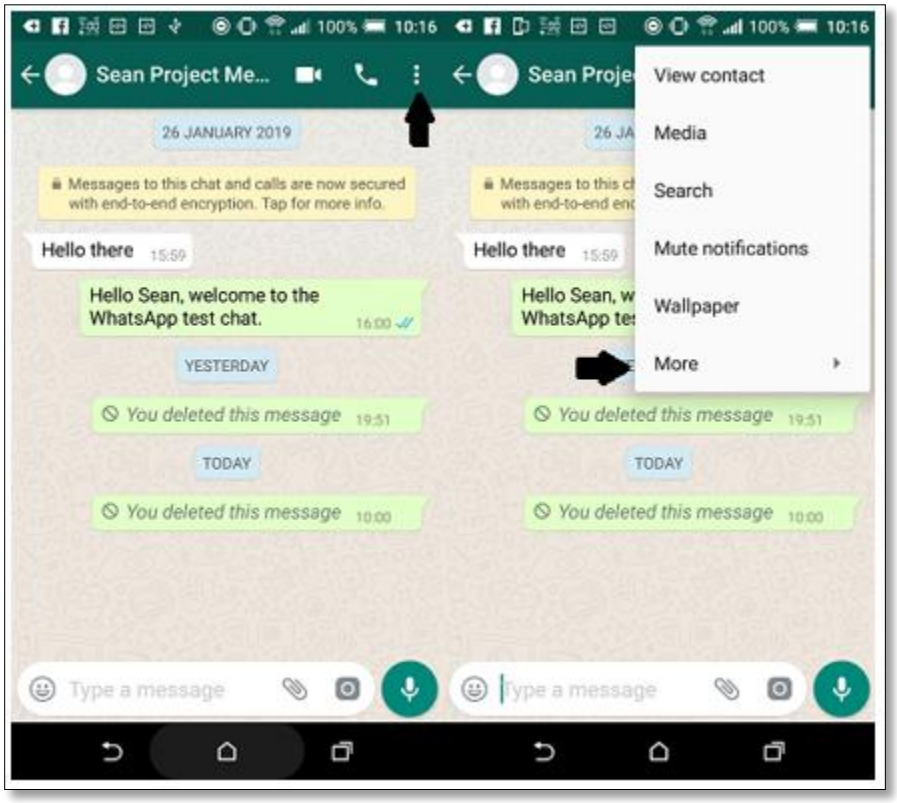


Figure 138 Here we see the chat options being selected via the 3 dots, followed by the more option setting.

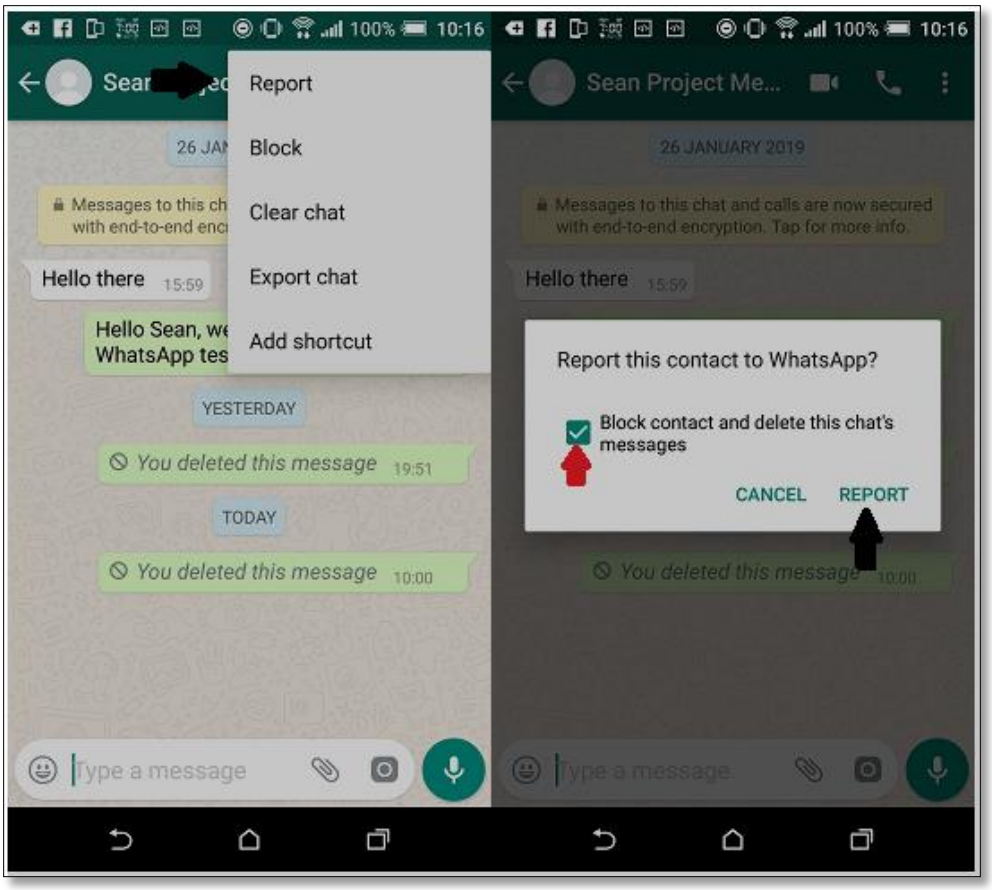


Figure 139 Here we see the 'Report option being selected.

11.3.10 WhatsApp Best Practice Settings Guide

Having reviewed the settings, we will now offer a best practice guide to the settings we suggest be employed to better protect the child's use of their Apps and their device to increase their safety while accessing online content via Apps:

- Profile Picture: We recommend that a user's profile Photo be set to be seen by only those contacts you trust. Best practice would be to have it seen by nobody. In the case of a child, we do not recommend the use of a real picture.

- About: We recommend that users about information be restricted to only trusted users, and a child's should be restricted to nobody.

- Last Seen: Once again, this should be restricted to trusted users online. As with the previous settings, a Childs should be restricted to nobody.

- Status: we recommend this setting be set to those individuals such as family or friends who are trusted.

- Live-Location: As with all GPRS based services, we recommend that this be turned off, especially for children.

- Read recipients: this can be turned on or off. The only real use for this is for a user to hide when they are actively online or not.

- Security Notifications: We always recommend that this be turned on. While the encryption used within WhatsApp is safe, no encryption is 100% safe and secure. User should always be aware when the codes change between chats. Should the code change we recommend contacting the user by some other means, for example a phone call, to ask if something has changed. A reinstallation of the App or a change of phone for example.

- Two Step Verification: While it will most likely ensure that Adult intervention is needed whenever an account needs to be verified, we do recommend this setting fully utilized with a strong password. This will ensure that the account in question cannot be downloaded and accessed by other users.

- Chat Backups: We recommend that external chat backups not be used as they increase the likely hood of data breaches leaking information such as phone numbers and email addresses which make it more likely that inappropriate contacts may contact you, or your child. This setting should be set to 'Never'.

11.3.11 WhatsApp App Safety Rating

Based on our custom App safety rating system and our best practice guide being fully implemented the WhatsApp App scores as follows.

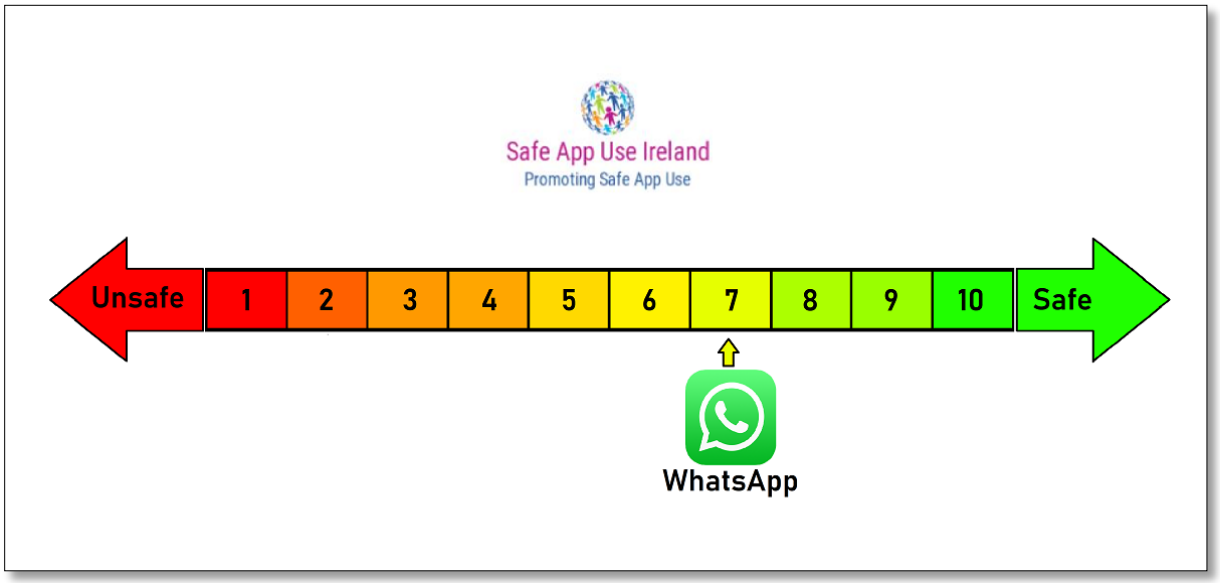


Figure 140 For Breakdown of Points System, please see: 10.0 App Safety

11.3.12 Reflections on WhatsApp

All things considered we find WhatsApp, with the proper precautions to be a relatively safe App when compared to other similar products. The End-to-End encryption, while not flawless, provides an acceptable level of security and peace of mind for parents. However, we must stress; no security ever replaces the strict monitoring of a child's online activity by a parent. WhatsApp security procedures and features simply ensure peace of mind for a parent during those times when a parent cannot be there to supervise.

The lack of ability to search a user is a very useful feature from the perspective of parents and it precludes the possibility of predators executing random, or automated searches. Mass spam messaging for solicitations are also prohibited.

The ability to remove messages from both ends of a conversation is useful too as no child is perfect and might occasionally slip up and share inappropriate personal info or other data. Unlike most Apps, WhatsApp allows a parent to clean up a child's accidental spilling of information.

The ability to restrict the collection of or sharing of personal data is perhaps more extensive than in most Apps of this nature. It is not perfect and most likely no App ever will be, however, the quality of life and peace of mind features provided are particularly good from the perspective of both child and parent users. Where proper security settings are applied we consider WhatsApp to be a relatively safe App for both parents and children.

11.4 YouTube / Google Family-Link / YouTube Kids

11.4.1 YouTube

YouTube is the most popular online video sharing site in the world with 1.7 billion monthly active YouTube users, and 300 hours of videos uploaded per minute **(Omnicoreagency, 2019)**. On YouTube users can view videos without signing in, however, videos that have been flagged as inappropriate for younger audiences require you to be signed in.

To create an account, you must create a Gmail Account due to YouTube now being owned by Google. If a person is under the age of 13 when creating a Gmail Account, a parent must sign in using their Gmail account to give consent that their child can use the service, however, they must use YouTube Kids which is an App specifically designed to be child friendly. There is a further Google security App that will need to be downloaded onto both the parent's and child's devices called Family-Link which allows them to control what their children have access to with other features such as how long they are allowed on their phone. **(Google, 2019)**. Although this is a very useful to protect your kids online, many parents don't know about this App and when children sign up all they must do is lie about their age and they can use it as if they were an adult. According to The Guardian, "more than 80% of children lie about their age to use sites like Facebook" **(Sweney M., 2013)**.

11.4.1.1 YouTube and Google's Terms & Conditions

YouTube is owned by Google and you must have a Google Account to make a YouTube account. As such,

- You must accept the terms and conditions to use YouTube features and services and acceptance of the terms is acceptance of all terms and stipulations therein. The terms for a legally binding contract between you and YouTube.

- Content creators, which is anybody who uploads to the service, are also subject to the terms and conditions, as is their data.

- You agree that the user will be solely responsible to YouTube and others for all activity that occurs under the users YouTube account. You further agree that users are solely responsible for any breach of the user's obligations under the terms and conditions and the consequences including any damage YouTube may suffer, for which YouTube shall be held responsible.

- You must set up a YouTube account to use some YouTube services and you must provide all required accurate information.

- Repeat infringers of copyright protections will be banned.

- You will not post unlawfully held or obtained material including material in breach of copyright. Posting of content implies you have the appropriate rights.

- YouTube reserves the right to remove inappropriate content that is found to breach any of the terms and conditions of service.

- YouTube may end its contract with users if they breach the terms or have behaved as if they intend not too or are legally required to do so.

11.4.1.2 Age Limits

You may not accept the Terms and conditions if you are not of legal age to form a binding contract with YouTube, which in Ireland is 13 years of age, or you are a person who is barred , prohibited or otherwise legally block from receiving or suing the service under the laws of Ireland; OR from the country which you are in when using the service.

11.4.1.3 Privacy Policy & Data Sharing

- The privacy policy covers what YouTube does with your data.

- All users agree not to attempt to harvest any personal data of any users of the service or website, including account names.

- Users including companies are prohibited from using emails to contact users for the purposes of solicitation.

- You retain the rights to your content, but limited license is extended to both YouTube and other users.

- YouTube does not guarantee confidentiality to any user content submitted.

- You understand that users are solely responsible for any content the publish and the consequences that go with it. YouTube does not endorse user content simply because it is posted.

- When you post content to YouTube you grant worldwide non-exclusive royalty free transferrable rights to use, copy, make derivatives of, display and otherwise distribute your content. However, you also grant these rights to other users! If you remove content that is visual such as video or audio, these rights are removed, however text content, such as content rights are granted permanently.

- You may not download content from YouTube that you did not upload.

- Third party's links to content or services or websites outside YouTube are clicked at the user's risk, and YouTube assumes o responsibility for any content or damages caused by content on such links.

- If you wish to end your legal user contract with YouTube, you may do so any time by writing to YouTube at the address above and closing your YouTube account.

- Google collect a wide variety of data types such as search history, videos watched, views and interactions with content and ads, voice and audio when audio features related to google services are used, purchase activity, people with whom you communicate or share content, activity on third party sites, Apps that use google services, and chrome history you've synced with your google account. Naturally uploaded content is stored also. Personal information such as name, address, email and phone number may also be collected. Personal information is not shared with partners.

- Users with whom you share personal data, such as our email address, may gain access through publicly available data, to other personal information, such as your full name and profile picture.

- Data relating to location via GPRS & GPS, IP address, sensor data and other device data and information relating to IOT devices such as WIFI Access points cell towers and Bluetooth enabled devices are also stored. As part of its search engine functions google may also collect publicly accessible information such as newspaper articles.

- Google will seek user's permission before using any data not covered by the privacy policy.

- Cookies, pixel tags, local storage, browser web storage, App cache data, databases and server logs are all used to collect this data.

- Google provides a feature to control what other see about you. This is access by logging into your Google account.

- This data is used to improve services included personalized add services.

11.4.1.4 Data Processing Terms

During the term of a contract if no option is provided to delete user data, YouTube will comply with any reasonable request to facilitate such deletion in so far as this is possible considering the nature and functionality of the pre-processor (YouTube) services. Google may charge a fee for this service. This fee will be calculated, and the user will be notified of the fee prior to the deletion.

When a contract ends all user data will be deleted within a reasonable time frim except where law prohibits it, or a customer request the data remain even after end of contract.

YouTube will upload and process any content uploaded in accordance with the data processing terms, except in cases where you uploaded such content for personal purposes or household activities

11.4.1.5 Abuse and Behaviour

- You agree to abide by all community guidelines.
- You acknowledge that in using the service, you may be exposed to content that Is factually inaccurate, offensive, indecent, or otherwise inappropriate or objectionable to you.
- You agree to waive, and hereby do waive, any legal equitable rights or remedies you have against YouTube with respect to any such content.
- Nudity, sexual content and/or pornography is prohibited. Any Exploitation of children will be reported to the appropriate authorities immediately.
- Harmful or dangerous content such as encouraging other to hurt themselves or videos containing self-harm may get age-restricted or even removed.
- Unwanted sexualization is prohibited.
- Unauthorized recording of users is prohibited
- Hateful content towards those of certain ages, genders nationalities, veteran status or sexual orientation/gender identity, racism, religious hate; or discriminating against those with disabilities or condoning violence against any of the after mentioned is prohibited.
- Violent or graphic content and/or gory content that's intended to be shocking, sensational or gratuitous is not okay unless it's in a documentary or educational manner. If posting such content, it should be accompanied by enough information to explain the purpose of the posting and the content from a documentary or educational standpoint.
- Harassment and cyberbullying are strictly prohibited including comments designed to be abusive. Such behaviour can and should be reported and it will be investigated and if necessary acted on.
- Spam, misleading data/metadata and scams are strictly prohibited. This includes titles, tags, descriptions and thumbnails. Spamming of content and comments is almost prohibited.
- Threats, which includes predatory behaviour, stalking harassment, intimidation, invading privacy and/or revealing other user's personal information and inciting others to do the same or commit violent acts is a serious breach of the terms and conditions and will be acted upon very seriously. Users who commit these acts will be banned and reported to the proper authorities.
- If a user violates your privacy and post your personal information this can be reported, and you can request the information be removed and report the user.
- Accounts created to impersonate somebody, such as a famous persona are subject to being removed without warning if it is discovered you are falsely claiming to somebody they are not.

- YouTube considers a child to be any user under the legal age of majority which in most countries is 18. All child safety guidelines are aimed at all such users.

- Any videos containing footage of children in sexually compromising situations such as sex abuse imagery, even those displayed for documentary and/or educational purposes, are reported to the National Centre for missing and exploited children who work closely with law enforcement.

- Content contained children in dangerous or harmful situation may be removed and/or report as appropriate as well as a potential strike being placed against the posting account.

- If any content is found to have placed a child in danger YouTube will work with law enforcement to assist all investigations by law enforcement.

11.4.1.6 Security

- Where possible Google will notify users of a data breach immediately including all relevant information pertinent to the breach. This is not an admission of fault of Googles part.

- The customer is solely responsible for the use of their account and the security of their account while using the services.

- Google is not responsible for the security of data transferred to any third party via the services.

- Use of the services is an acknowledgement that the security set in place by Google is appropriate to the services being provided.

- Users may request a security audit of YouTube via Google but may be charged a fee for doing so.

11.4.1.7 The Nature of Data Collected

Unlike other Apps, YouTube by its very nature must collect data, both in terms of user details pertinent to account creation, integrity and security, but also that which the user uploads. That is the whole point of the service. Any audio visual or text-based data is collected and stored by YouTube.
YouTube/Google will also collect analytical data relating to how, when and where the service is sued to improve service and help business maximize the effectiveness of the service.
Data is stored and shared globally and may be stored on any of googles data centres.

11.4.1.8 YouTube Features

Once you have created your account the home page of YouTube will show up. This page contains suggested videos based on your watching habits that people have uploaded on their channels. An example would be if you watch many DIY videos then you may find a lot of those being recommended.

To show the functionality of YouTube as a new comer we made a new account and named it David Murphy. Below is a screenshot from the YouTube App after creating our account. What is shown on the Home tab is a list of videos that I can scroll through from music videos to homemade dog videos. At the top right you can tap on the magnifying glass and search for videos by name or topic. The icon to the left of the magnifying glass allows you to send videos to a smart tv nearby. On the bottom of the screen is the different sections of the App. "The Trending page helps viewers see what's happening on YouTube and in the world. Some trends are predictable, like a new song from a popular artist or a new movie trailer. Others are surprising, like a viral video. Trending aims to surface videos that a wide range of viewers will appreciate." **(YouTube, 2019)**.

The next tab is the subscriptions tab. The way subscriptions work is if you like a creator and want to see more of their stuff you can subscribe to them and then you will be kept up to date on their uploads. The subscriptions tab is where YouTube stores the people you subscribe to and shows their latest uploads.

The inbox tab is where YouTube stores your notifications and messages people have sent you. People can only send you messages if you are friends with them on YouTube. To add friends, you must go into inbox and select "Add Friends" and send them the invitation code. The last tab is the library tab. This is where YouTube stores your viewing history, videos you've uploaded, videos you've purchased and videos you've added to playlists.

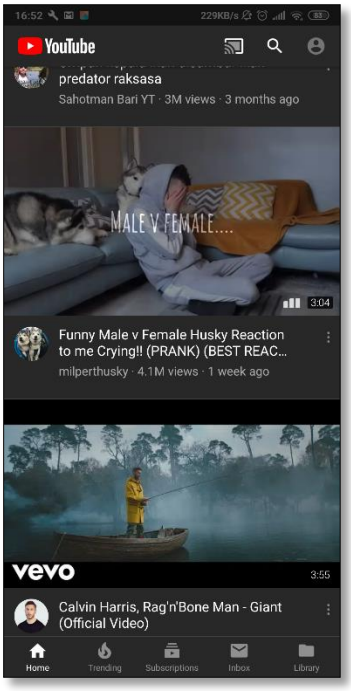


Figure 141 The home page of YouTube.

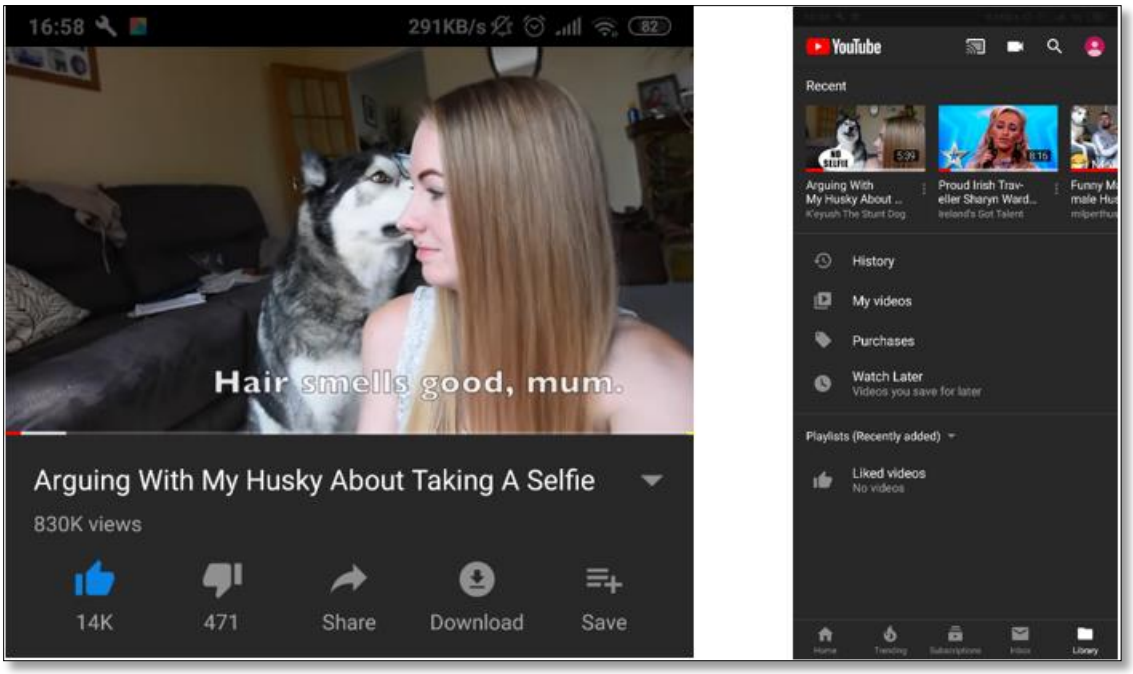


Figure 142 On the left we see the liking feature and on the right, we see the Library tab.

You can add videos to your liked videos by clicking the thumbs up button. You can also press save on a video as shown below to add it to a playlist or share it to other social media sites like Facebook. You can also dislike a video if you don't like them.

There is also a download option on videos which allows you to download the video if you have YouTube Premium. YouTube Premium is a subscription-based service which gives you more features like downloading videos and no adds will show up on any videos. There are also YouTube Premium videos like the TV Show Mind Field by the content creator Vsauce. YouTube Sponsors the channel to create the videos in a Tv-Series style with different episodes and then to view them you must subscribe to YouTube premium.

YouTube also has their own TV Network called YouTube TV which is a cable-free live TV service for $40 a month although its currently only available in the US now **(YouTube, 2019)**. YouTube also has a movie streaming service called YouTube Movies where you can buy or rent movies **(Gonzalez B., 2019)**. Another feature of YouTube is YouTube Gaming. It is a feature that combines popular gaming videos together in one place along with live videos currently being played. This feature is going to be shut down soon however.

On every YouTube video by default there Is a comments section. This is where people who have watched the video can leave feedback or comments on what they like, dislike, or generally think about the video. People can then respond to these comments and create dialogue between other users on YouTube about the video and start a discussion. By default, anyone can reply to anyone's comment and see anything anyone has commented. Comments can also be liked and disliked by everyone who sees them. Once posted comments can be edited or deleted by who made them.

As of 2016, YouTube has been added to Googles HTTPS Transparency Report, this provides encryption to the service for any devices that support TLS (Transport Layer Security) encryption, as a result all privates messages shall be encrypted, however comments being public will not be encrypted **(Schechter E. 2016)**.

My Channel:

On YouTube every user is given a channel. Here they can upload videos, share playlists they have made of their favourite videos on YouTube. By default, only you can see your liked videos and subscriptions however everyone can see the videos you add to a playlist like the one shown below in the Favourites playlist.

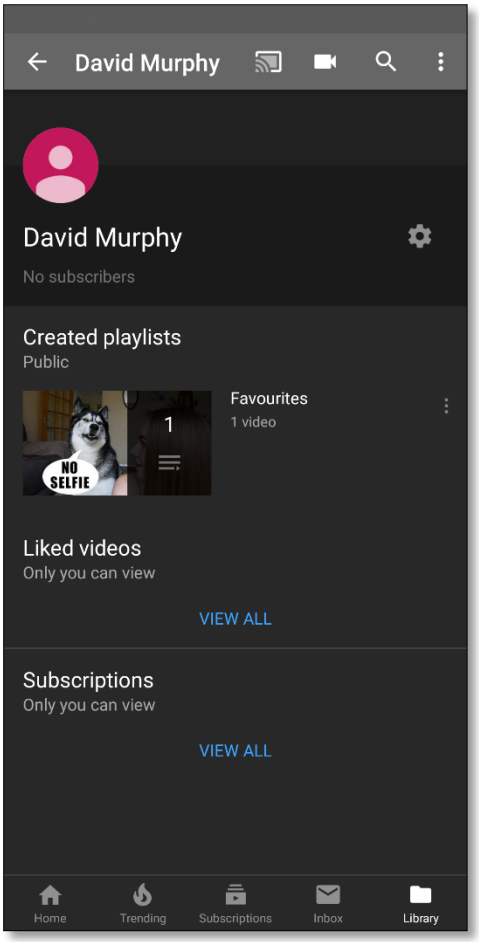


Figure 143 My Channel Page in the Library Tab

11.4.1.9 YouTube's Personal Security Optimization Options

Here are the security settings available for YouTube:

- Manage Restricted Mode
- Manage contacts

Below are the options available further on the Google account required to use YouTube:

- Google profile visible
- Manage 2-step verifications
- Manage Shared Endorsements
- Manage account plans

In the next section we will detail how to perform these actions in detail.

11.4.1.10 YouTube Settings

If you have an account on YouTube, you can go into the settings and turn on Restricted Mode. This helps hide videos with potentially mature content however it is important to note that it is not 100% accurate and some videos may slip through the cracks.

To enable this setting, press the profile icon as shown on the left in figure 126, on the next page tap on Settings as shown on the right in figure 126, on the next page tap on General as shown in figure 8. On this page, enable the setting "Restricted mode" as shown on the right in figure 127.

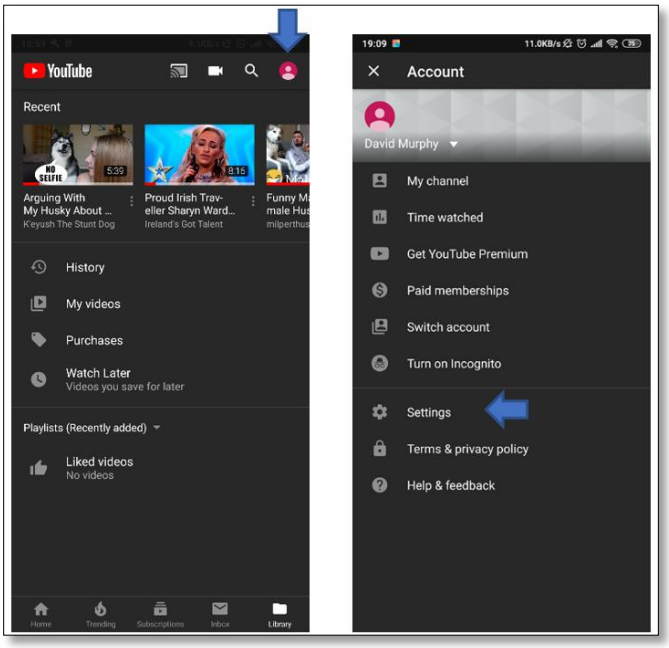


Figure 144 Locating the Settings.

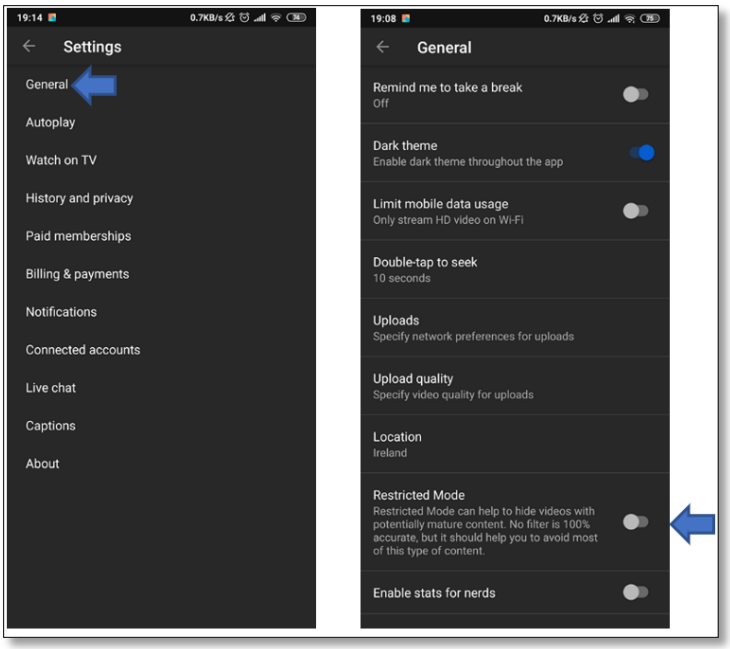


Figure 145 Locating Restricted Mode in General Settings

If a user sends you inappropriate messages you can block them using the block feature on YouTube.

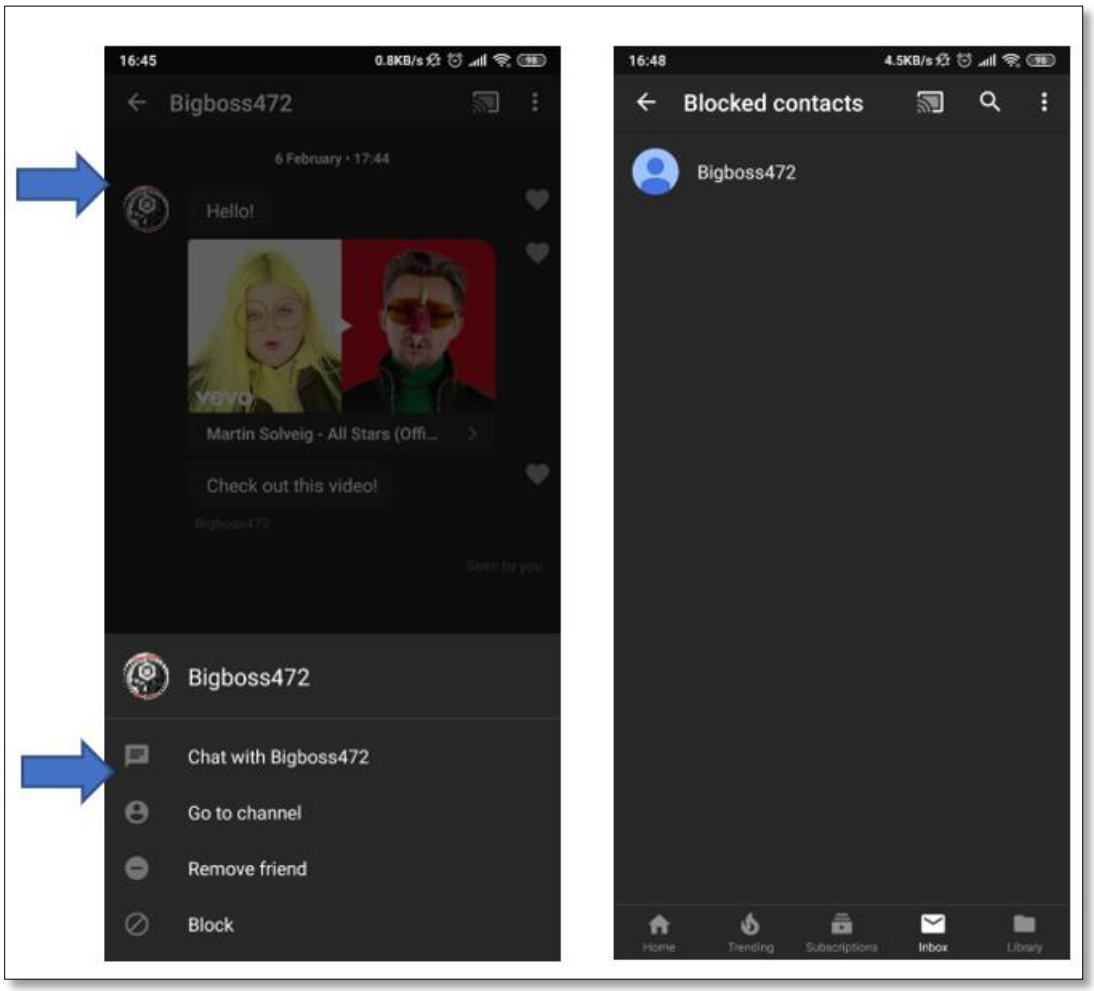


Figure 146 Blocking a User on YouTube.

Just tap on their profile Icon and click Block to prevent them from messaging you again. Now the blocked person will show up in your "Blocked Contacts" section of your settings and can be unblocked there if needed.

11.4.1.11 Securing the Google Account

To create a YouTube account, you must have a Gmail account. To be fully safe in using the App you must understand and select the safety features that you would like to have for not only YouTube but your Google account too.

To begin configuring your Google account you must go to your Google Account at myaccount.google.com and sign in, you will then be at the home page for your account. To begin securing the account, click on "Data & personalisation". Here you can configure the Activity controls on your account. For this example, we used a test account.

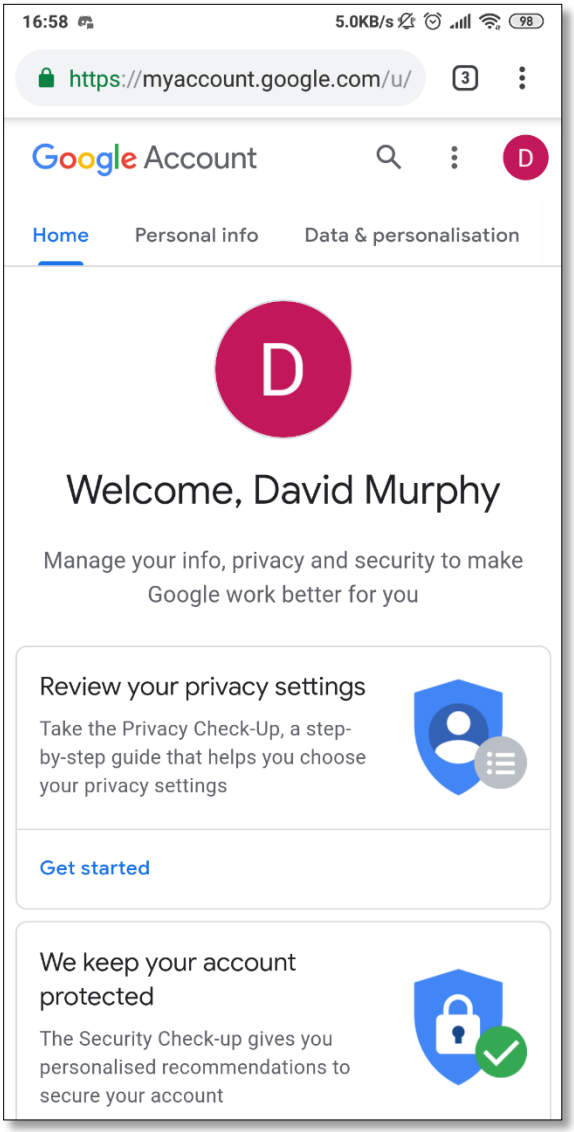


Figure 147 Home page of David's Google Account

Below is the information on the activity controls provided by Google **(Google, 2019)**:

- Web & App Activity
  Google is saving your activity on Google sites and Apps, including searches and associated information. Google is also saving activity as which Apps you use, your Chrome history and which sites you visit on the web.

- Location History
  Google creates a private map of where you go with your signed-in devices, even when you aren't using a specific Google service. This map is only visible to you.

- Voice & Audio Activity
  When you use voice commands or touch the microphone icon, Google saves your voice and accompanying audio.

- Device Information
  Google is storing information about contacts, calendars, Apps, music and other data from your devices in your Google Account.

- YouTube Search History
  Google is saving your YouTube searches to your Google Account.

- YouTube Watch History
  Google is saving the YouTube videos that you watch to your account.

All the above settings can be Toggled on or off on the "Data & Personalisation" page as shown below

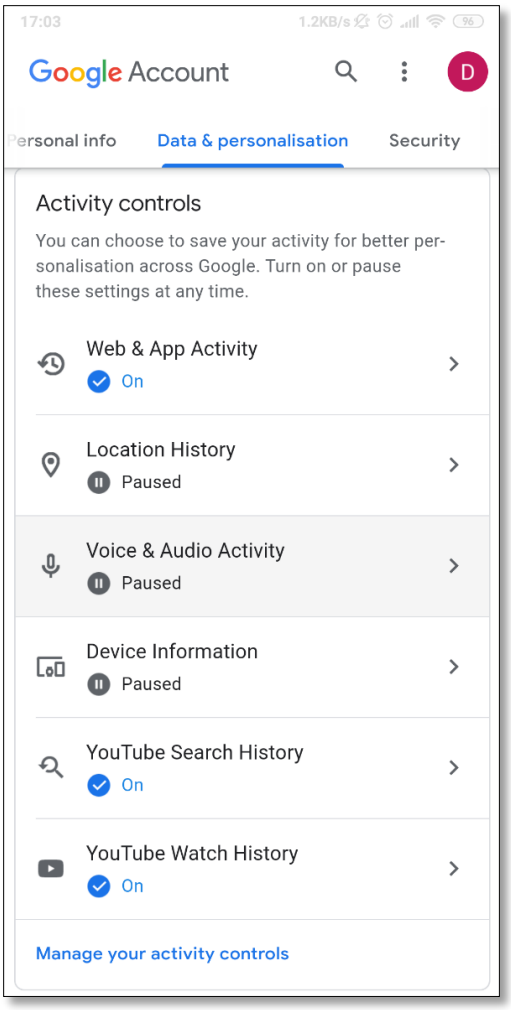


Figure 148 Data & Protection Tab in David's Google Account.

The next step is to make sure your account is secure. Go back to the Home page and tap on Secure account. As shown below. Your Google account allows you to set up an account recovery service. You will need to provide a recovery email or a phone number to set it up. This works if you lose access to your account you can request a link to reset your password to be sent to either your phone or your recovery email. Google also scans your device to check if there are any harmful Apps installed and warns you about them. It also tracks here the Recent security events that have taken place such as adding a phone number to your sign-in recovery or changing your password.

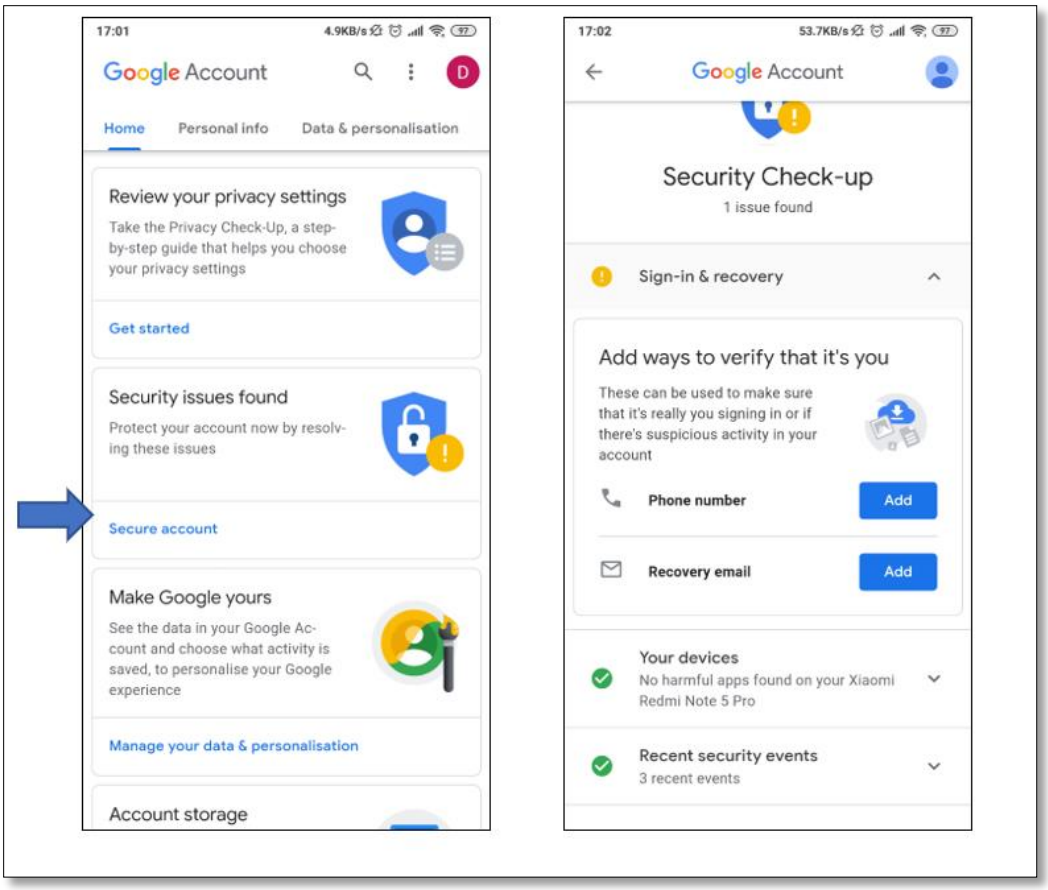


Figure 149 Viewing the Security Issues on David's Google Account.

Next, click on the Personal Info tab as shown below. Here you will be able to change your account info. If you scroll down to the bottom of this page you can view your account from the perspective of someone else.

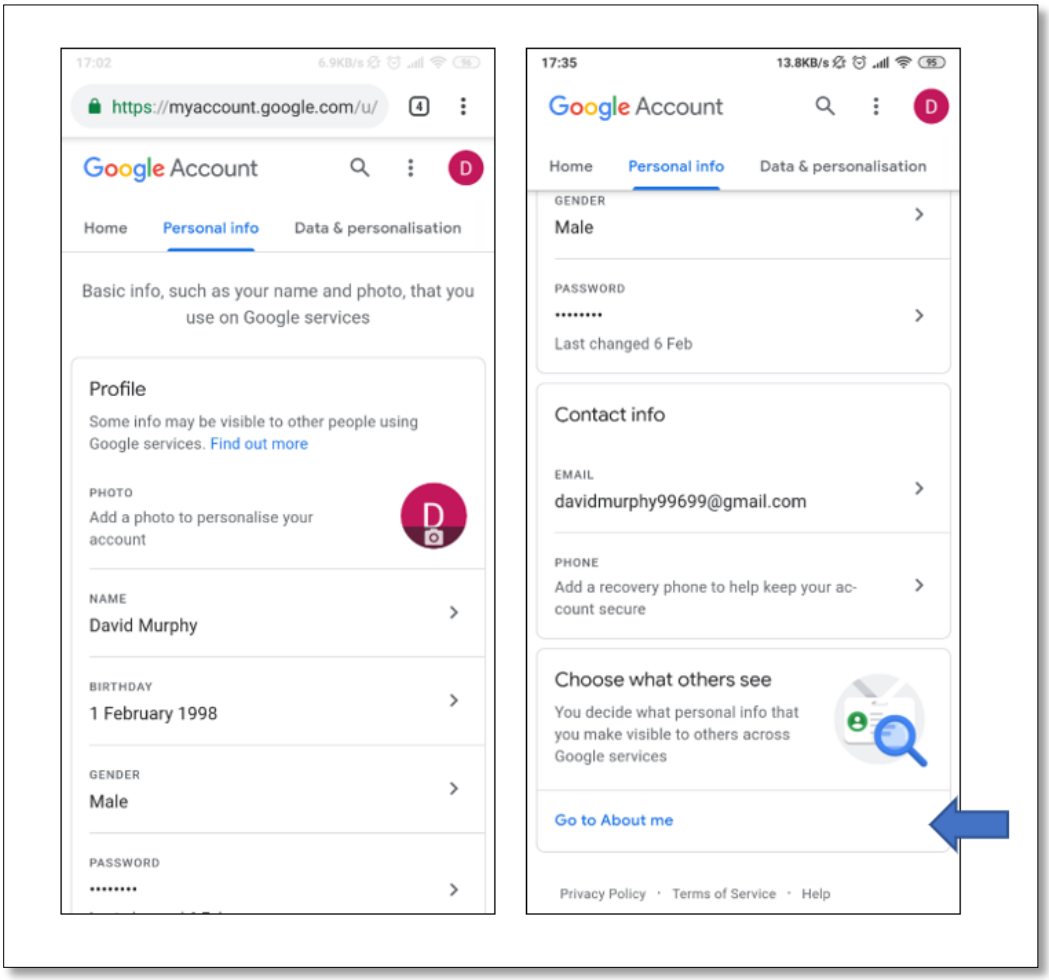


Figure 150 Viewing the About Me page of David's Google Account

In the picture below, we can see what an outside user may see about your account. The only things they can't see is the pieces of information that have a lock icon next to them as shown with the blue arrows. This information can be changed to visible if you tap on the lock and choose visible.

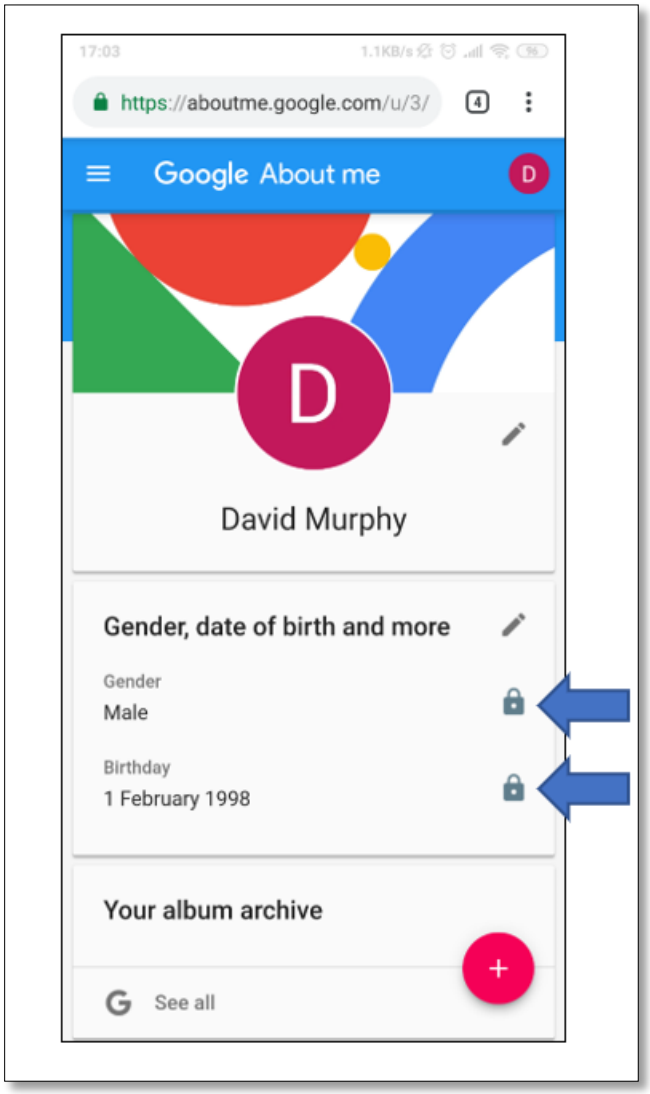


Figure 151 About Me page for David's Google Account

Finally, in the Security tab, you can set up your phone to allow you to sign into google without typing in your password. All you need to do is to allow the login on your phone, so you can log in on other devices without a password. You can also enable 2-step Verification which prevents anyone form logging in without having the password AND a second key that is sent to your phone. In this section you can also change your password.

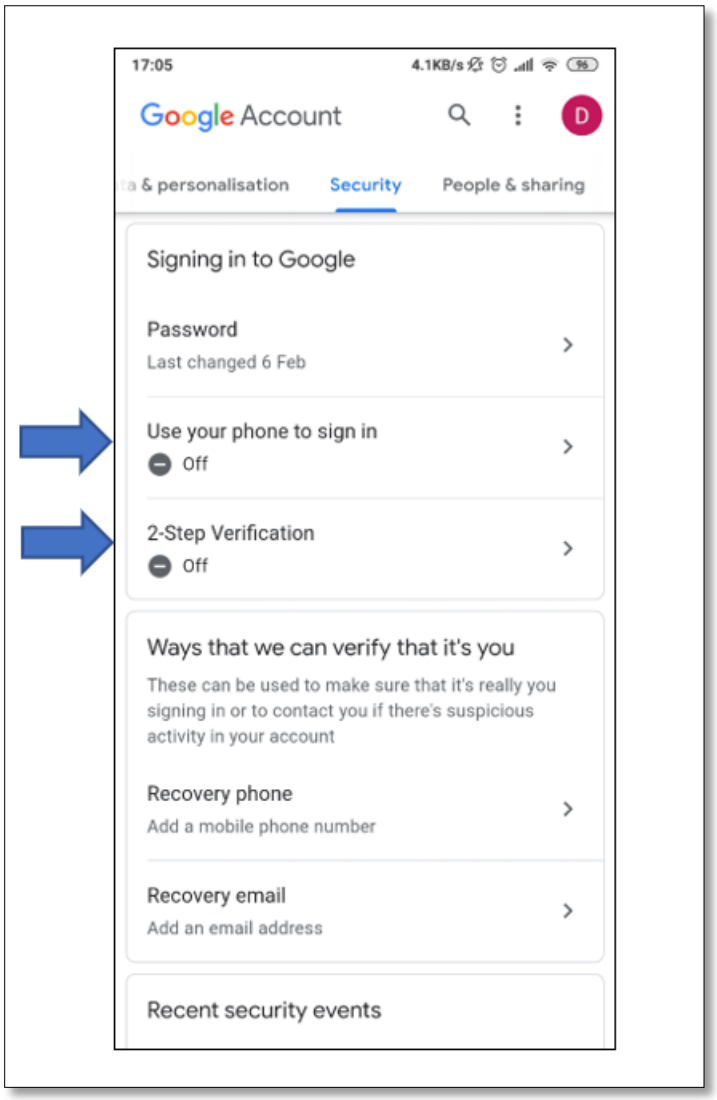


Figure 152 Security Tab of David's Google Account

Google does not share your data with any third-party company beyond their direct partners or a third-party hosting services contracted to Google, however they use your data for their ad services which is indirectly selling your data without revealing it **(Google 2019).** This is a great way to monetize the data they have on you without infringing on your privacy.

The next steps will show you how to download the data Google tracks when you use their services, plan for your account to be deleted upon being inactive from 3 to 18 months and you may delete a service on your account or all the information Google has on you, this will permanently delete your google account.

On the Data & Personalisation tab, scroll down until you see the following screen. To download your data, you must first request an archive to be created on your data, this could take a while depending on how much data they have for you but for the new account we created, we received an email just a few minutes after the request was made. The information was stored in a zipped file and must be extracted before read. To unzip this data, we used a computer with WinRAR.

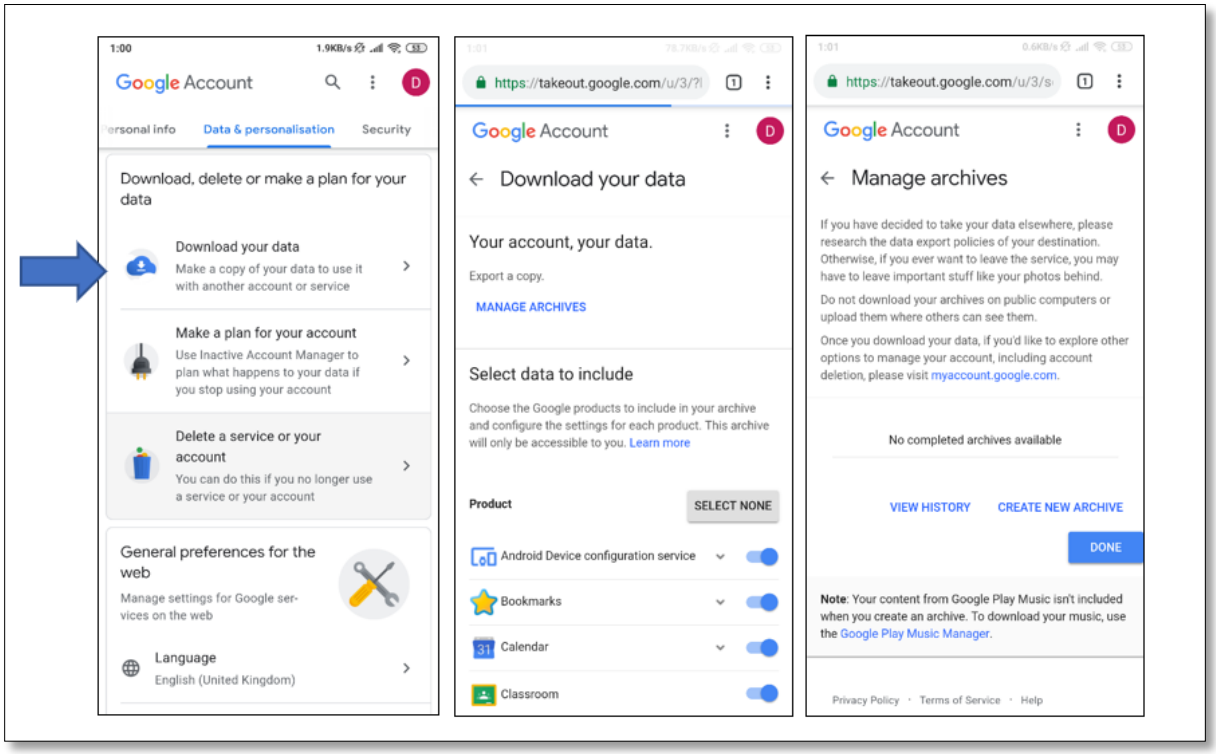


Figure 153 WinRAR Extraction of the Data Downloaded

The information contained device information, such as the contacts and their photos you have assigned to them on your phone and other things like bookmarks on your chrome browser.

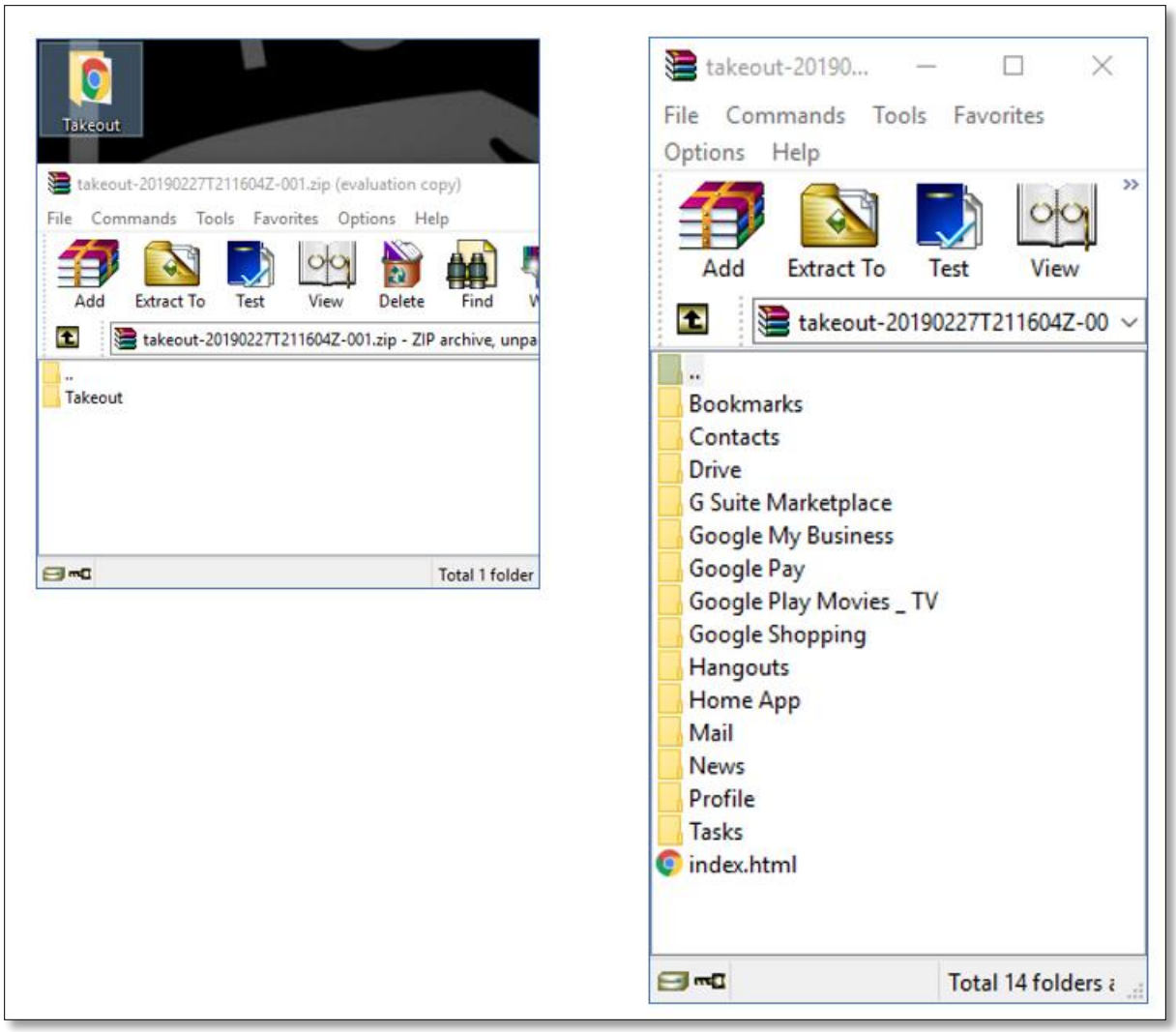


Figure 154 How to Download a User's Data.

The next option would be planning for your account if it goes inactive. It allows you to, after a specified number of months of inactivity, delete your account automatically. To set this up select the option as shown below. You will then need to give them your phone number and select how long to wait before deleting the account for its inactivity. Before it gets set up they will contact your multiple times by SMS and Email to confirm the changes and they will also contact you 1 month before the set time is up for extra care.

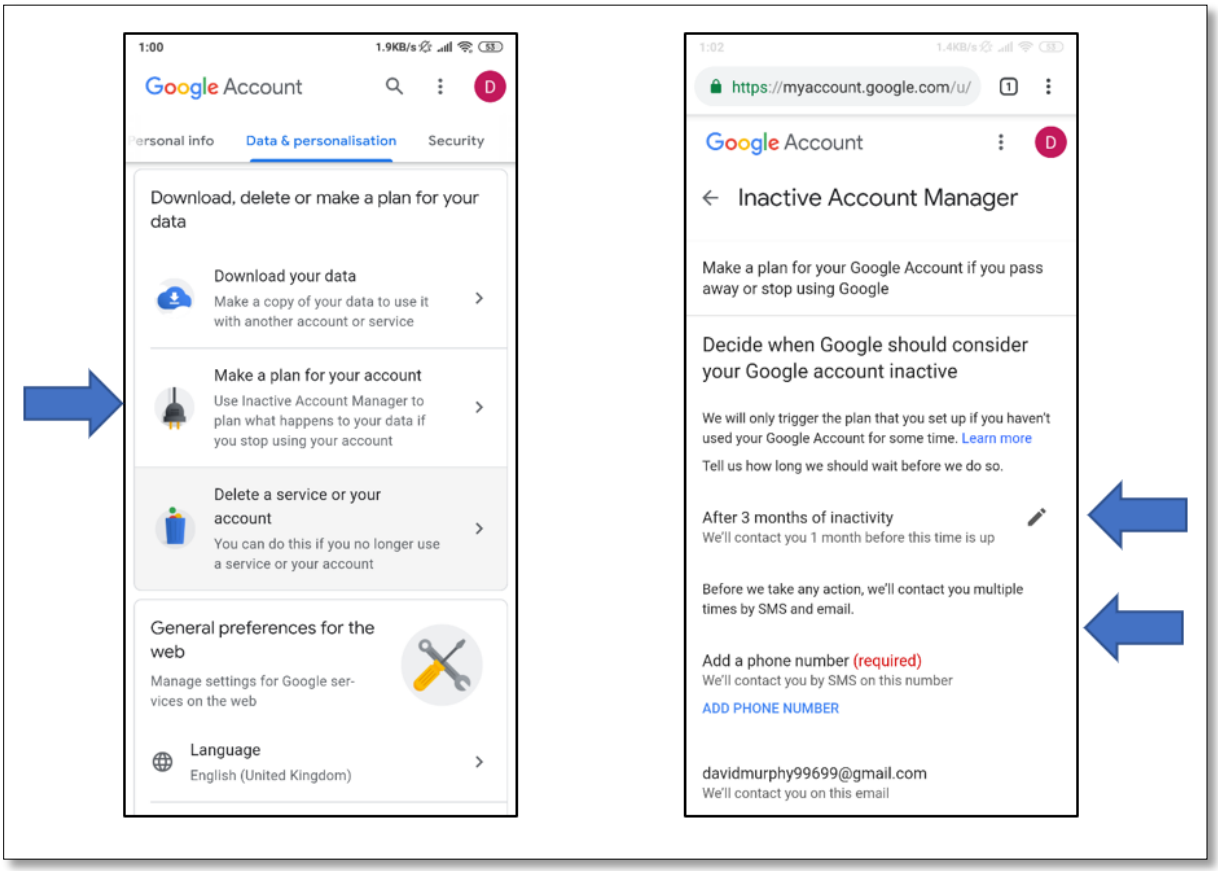


Figure 155 Making Plans for a Google Account

This final setting is set off by default however if used, the Shared Endorsements feature of Google could be used to gather information on the users. Shared endorsements are a feature that allows you to review places like restaurants and leisure centres like cinemas and swimming pools. However, it's important to note that if you enable this feature, then 'Based on your activity, Google may show your profile name, profile photo, and activity in shared endorsements in ads.'. If you want to make sure this feature is turned off, you must go to the People & Sharing tab and scroll down to the bottom as show below. Select manage shared endorsements and scroll down and make sure the box shown below is unticked.

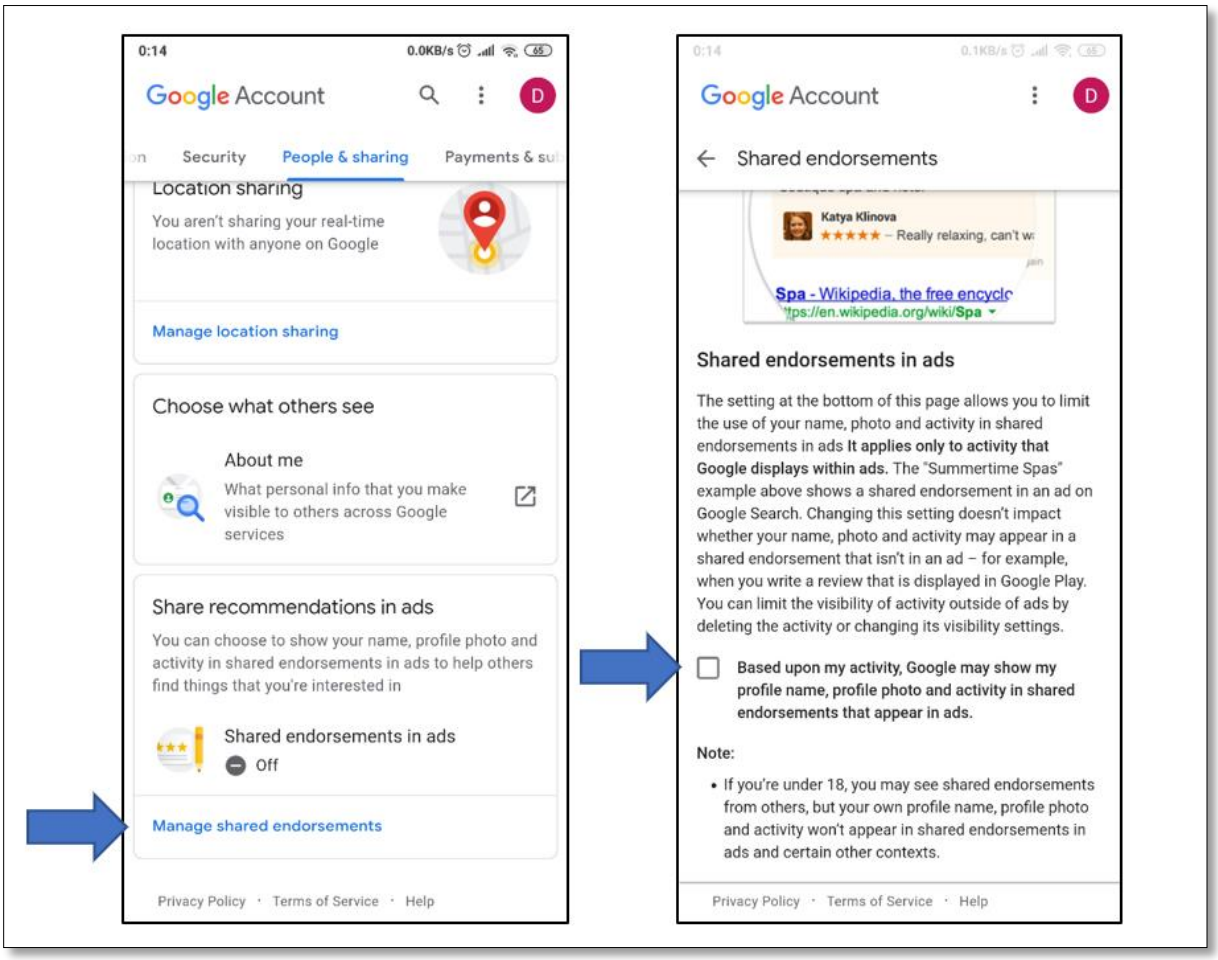


Figure 156 Managing a User's Shared Endorsements

11.4.1.12 YouTube Best Practice Settings Guide

Having reviewed the settings, we will now offer a best practice guide to the settings we suggest be employed to better protect the child's use of their Apps and their device to increase their safety while accessing online content via Apps:

- We Recommend enabling Restricted Mode to enable the filtering of potentially mature content however it's not 100% accurate.
- We Recommend disabling Web & App Activity
- We Recommend disabling Location History
- We Recommend disabling Voice & Audio Activity
- We Recommend disabling Device Information
- We Recommend disabling YouTube Search History
- We Recommend disabling YouTube Watch History
- We Recommend disabling Web & App Activity
- We Recommend disabling Web & App Activity
- We Recommend keeping all information of the account set to private as default.

12.4.1.12 YouTube App Safety Rating

Based on our custom App safety rating system and our best practice guide being fully implemented the YouTube App scores as follows.

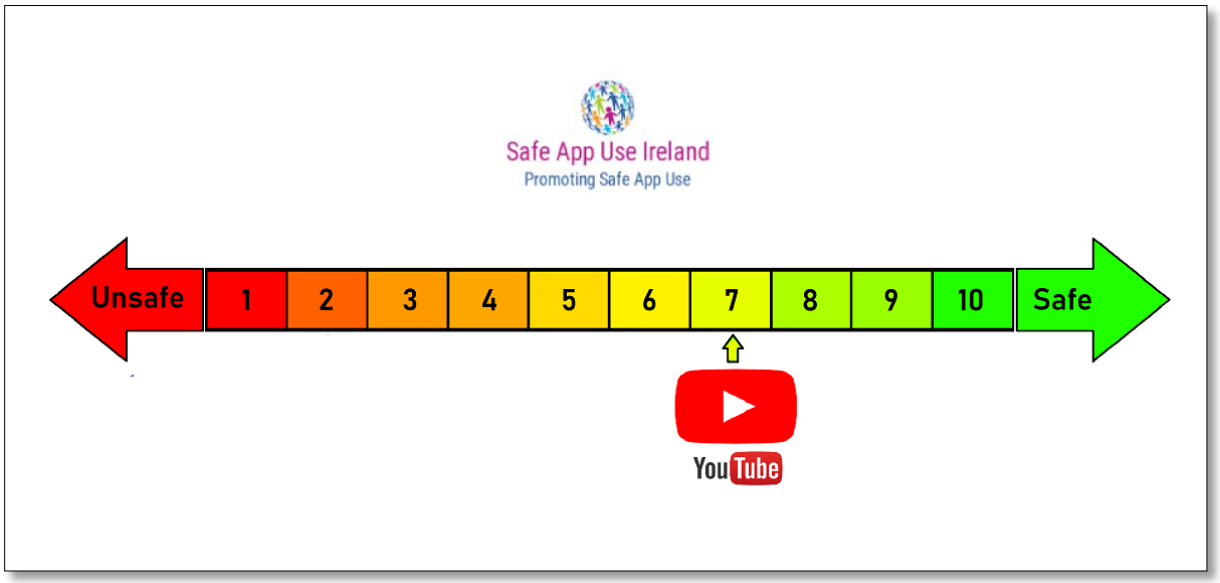


Figure 157 For Breakdown of Points System, please see: 10.0 App Safety

11.4.1.13 Reflections on YouTube

As stated by YouTubes terms & conditions, we do not recommend anyone under the age of 13 to use the main YouTube App for any reason, be it supervised or otherwise. The potential for the child in question to tap onto the inappropriate area that encircles the "Elsa-gate" videos. The algorithm of YouTube, been tasked with such a huge goal, has its flaws and may allow such things to be suggested to children despite their inappropriate nature.

Despite this, if used with the maximum extent of security options available, YouTube can be a safe outlet of entertainment for minors if supervised by a guardian and the appropriate settings are used. We do not recommend it for children. There is another Option we shall cover.

11.4.2 Google Family-Link

Our research into YouTube led us to the YouTube-Kids App. Which in turn led us to Google Family-Link. This requires a slightly different approach in terms of research then our previous Apps. Therefore, to ensure we are providing the best security recommendations from the perspective of a parent, we shall step back and approach this from in terms of a parent setting up an account from scratch on a new android device. This means it will be a lengthy process, requiring 3 steps as follows:

1. Set Google Accounts as needed, for parent, child or parent & child.
2. Set up Family Link account
3. Setup YouTube-Kids Account

For the purposes of our research we elected to use one of our group members Google accounts as a parental test account. We then set up a test child account.

It should be noted, that you cannot have a child account and an adult account on the same device.

Google Family-Link is a stand-alone security App which is required to be installed on the parents device and the child's device. It is also necessary to install Google Family-Link if a child under the age of 13 wants to create a Google Account. It allows users to manage their child's device and account activity. Its use extends far beyond YouTube, allowing the supervising adult to monitor device activity, location, use, grant and withdraw permissions, add and remove Apps as well as deleting a child's account, both locally on the device in question and remotely as needed. Multiple accounts can be managed via family groups, up to 6 members may be created allowing for multiple children as well as multiple supervising adults. Perfect for a family of 2 adults and 4 children for example. However, the user is not restricted to just one account, so, should more coverage for more children, or supervising adults be needed, more accounts can be created.

11.4.2.1 Google Family-Link Features

There are a few note-worthy comments to be made about Family-Link before we investigate its features and settings. While this a superb App, and Google deserve high praise for the security and peace of mind it affords parents, it is not fool proof. A tech savvy child may find ways around it, such as 'rooting' or 'jail-breaking' a phone. Unlikely as it may be, it is possible. Also, while the protections afforded are great, once a child reaches the age of 13, they are entitled to manage their own account and will be presented with the option to remove the parent account from managing their account with or without the parent's approval. This is beyond Googles control and is a legal requirement. However, with the recent amendment to Irelands digital age of consent raising he age limit to 16, this is something Google may wish to redress at some point. Finally, the number of family members that can be added to a family group is limited, so think carefully about who you invite to help manage or supervise your children.

So, what exactly is Family-Link, and what can it do? Family link, being an App that falls under the Google Umbrella, incorporates TLS (Transport Layer Security) encryption, which is now standard for all Google products **(Schechter 2016)**.

Family-Link is a stand-alone security monitoring tool for parents, used to monitor the online and device activity of children under 13 years of age. While it can be used beyond this age limit of course, children of 13 can bypass the restrictions simply by choosing to remove it.

Family-Link can track the child's device, activity and lock the screen. Denying access to prohibited sites (Accessed through google Chrome) or filtering potentially age inappropriate content is also possible. Denying the installation of inappropriate Apps is another feature offered. Almost every facet of the phones use can be remotely managed from the parent or supervisor's device.

Account settings, passwords, user details pertaining the child location setting's, and much more, can also be accessed and altered remotely. The child must request permission from the parent or supervisor to use any App, watch any video outside or allowed age ratings or visit any site that falls outside of the allowed parameters.

But there's one feature parents will love! Family-Link can set up time-based screen locks on the child's device. So, even if you're not there, and you say the child can have 1 hour of game time then homework takes precedence, you can be sure that the screen will lock after one hour without any intervention being required. The sheer scale of features and settings crammed into this App are impressive.

11.4.2.2 Google Family-Link's Personal Security Optimization Options

Below are the security features for Family-Link

- Manage Apps (restrict based on age rating, or remove)
- Manage Purchases (Prevent or allow)
- Manage Third Party Apps
- Manage location tracking settings
- Manage allowance of screen time (also set periods of allowance day/night mode)
- Manage Content (based on age rating)

In the next section we will discuss the way to enable and use these features.

11.4.2.3 Google Family-Link Setup

Upon choosing to create a new Google account, we are first presented with the option to create an account for yourself, or for a child (13 years old or under). As we have elected to use one of our group members accounts as our parent account we shall select the setup 'For My Child' option.

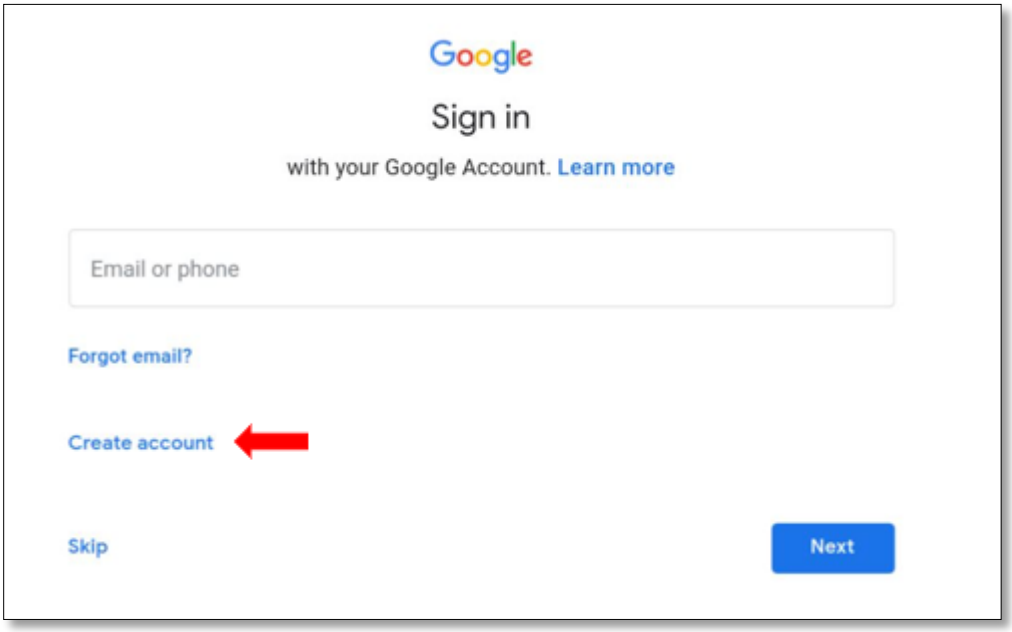


Figure 158 Here we select the create account option.

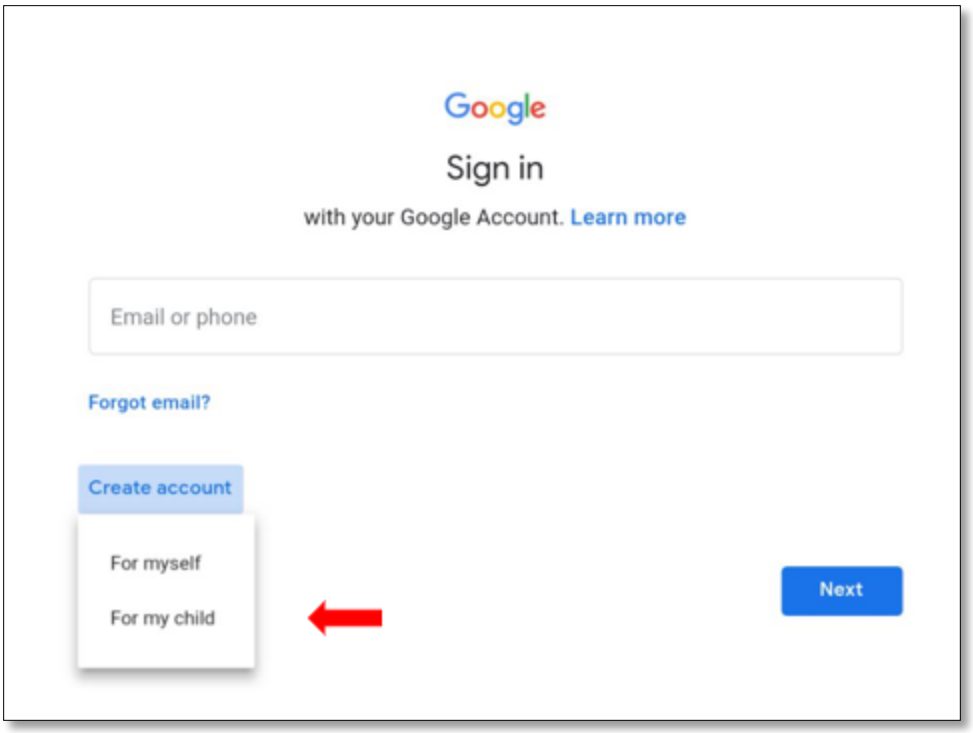


Figure 159 Now we select "For My Child".

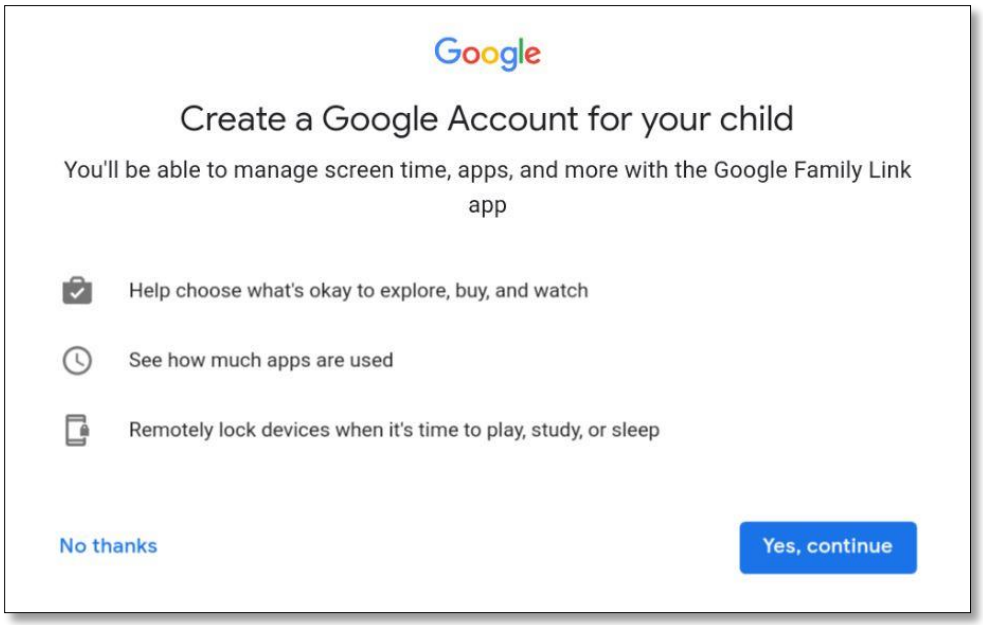


Figure 160 Here is a brief overview of the options available for parents in supervising your child's account, simply select "yes, continue".

Google will now send you a verification code to confirm you are not a BOT (automated program designed to maliciously set up accounts). Simply enter your phone number and select your international dialling code from the drop-down menu on the right as indicated by the red arrow.

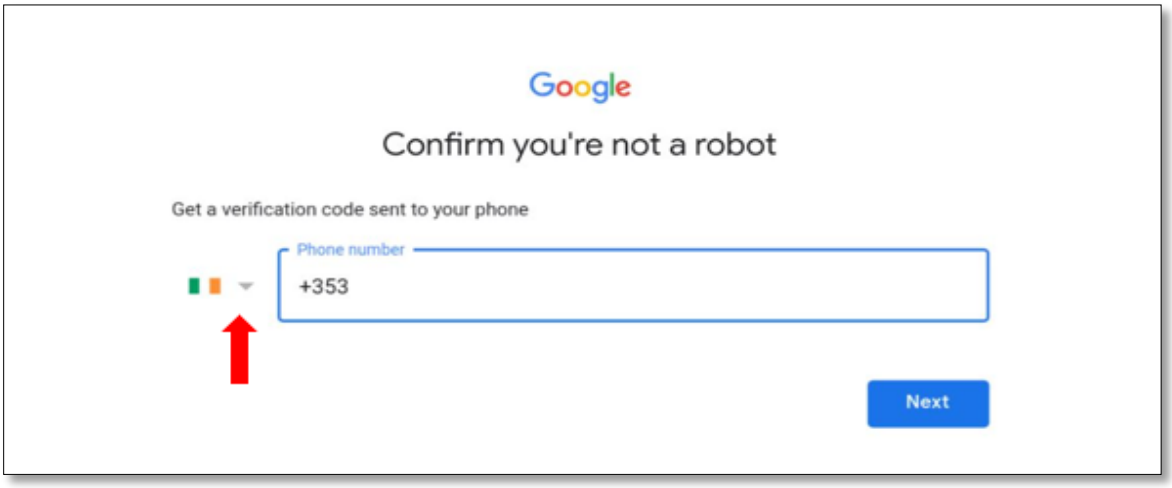


Figure 161 Enter your number to receive your verification code.

Once verified, you can begin to enter your child's information to set up their google account, as seen below.

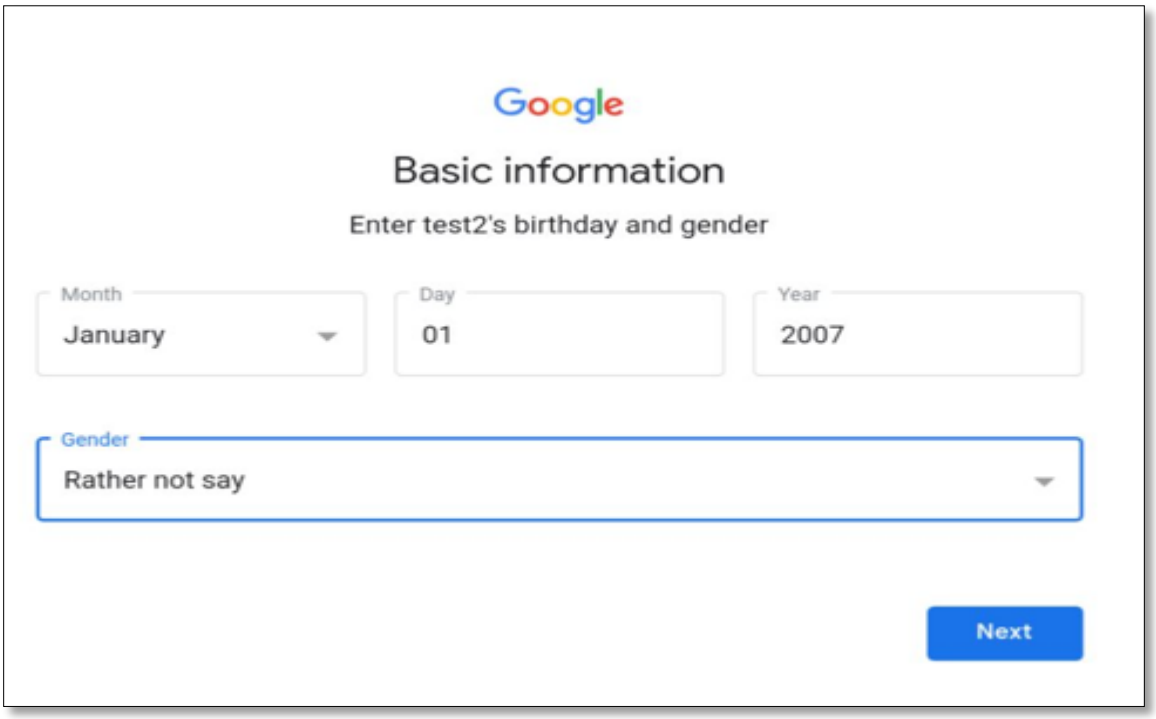


Figure 162 Now enter your child's date of birth.

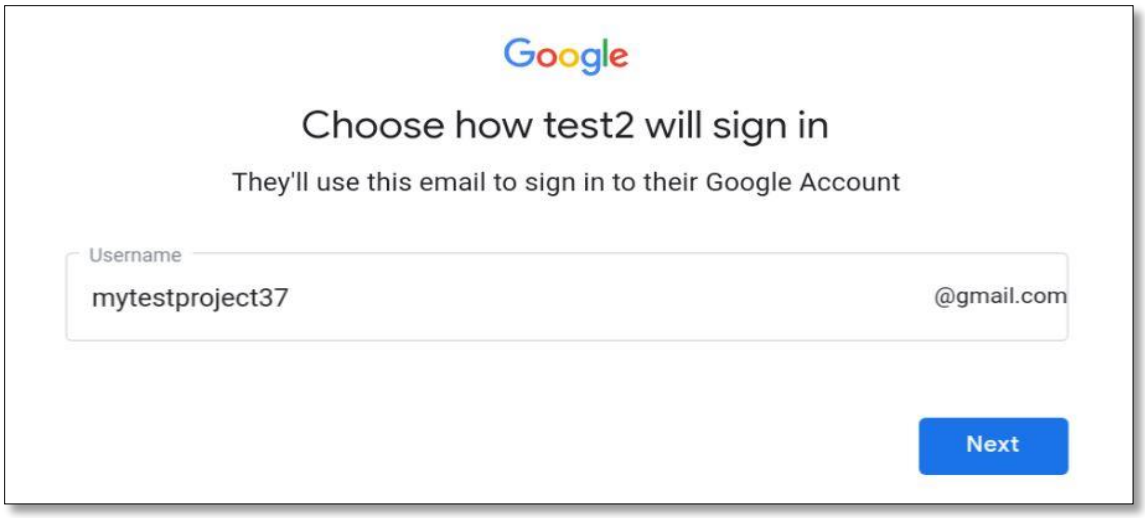


Figure 163 Chose an appropriate email account for your child.

Next, we will be creating a password for our child's account. This is a delicate area. There are two concerns here. Firstly, the password must be something the child can use. Secondly, the password must be secure such that it cannot be easily brute force attacked by a malicious user.

Current recommendations to avoid easy brute forcing is the use as random a string of text as possible. For a child we might use for example a book with a long title. We will also add in some "Leetspeak", where letters are substituted for numbers. Finally, we add in some random special characters and numbers. This way the password is somewhat familiar, and the child can easily develop mental muscle memory when it comes to entering the password. However, a reasonable level of security is maintained.

For example: "Harry Potter and the goblet of fire" would become "H4rry_p0tt3r_4nd_th3_g0bl3t_0f_fir3_1". The computational power required to brute force this password would be exceptionally high making it highly unlikely (though not impossible) to brute force attack this password.

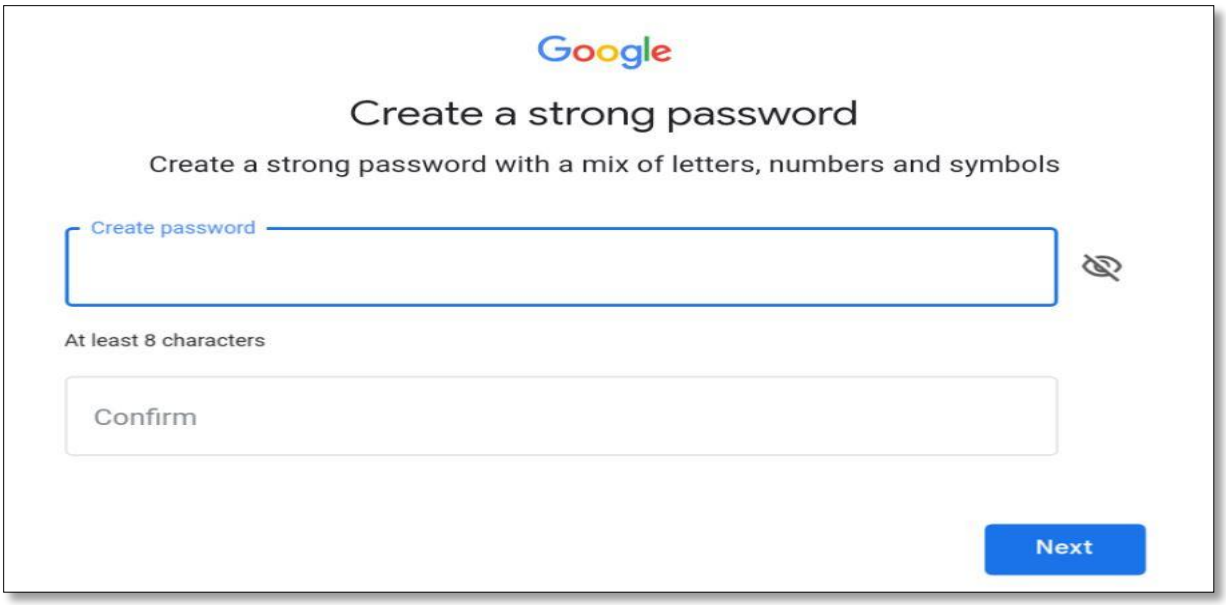


Figure 164 Enter an appropriate password, following the security recommendations above.

Now, we must sign in as a parent on our personal Google account by entering our email address and password.

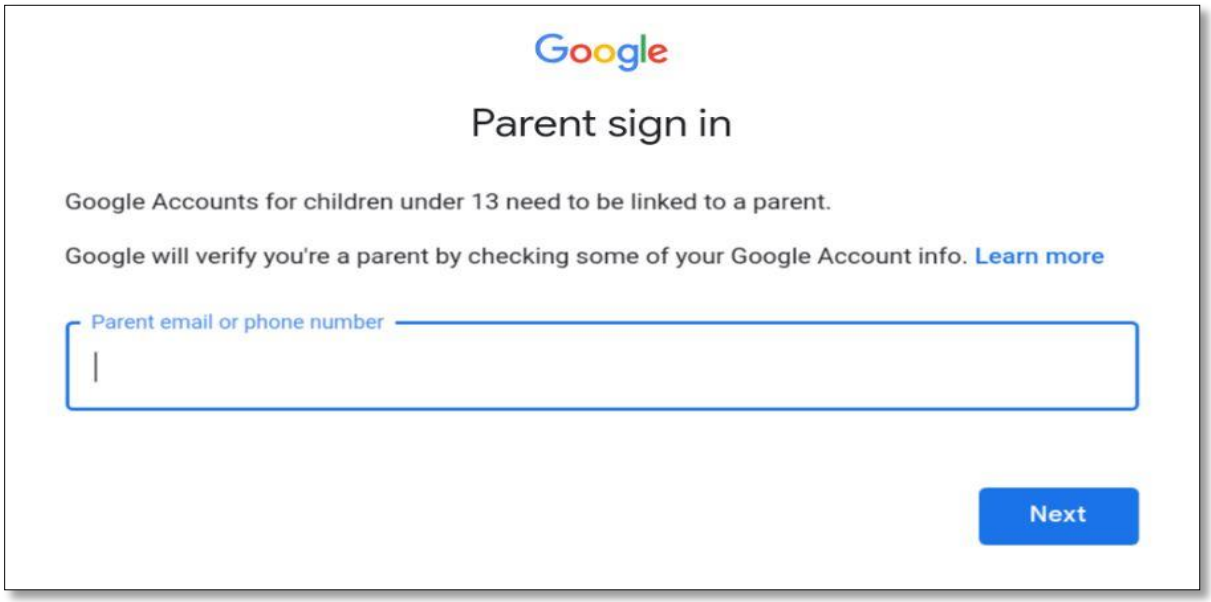


Figure 165 Now you must sign in as a parent on your own Google account.

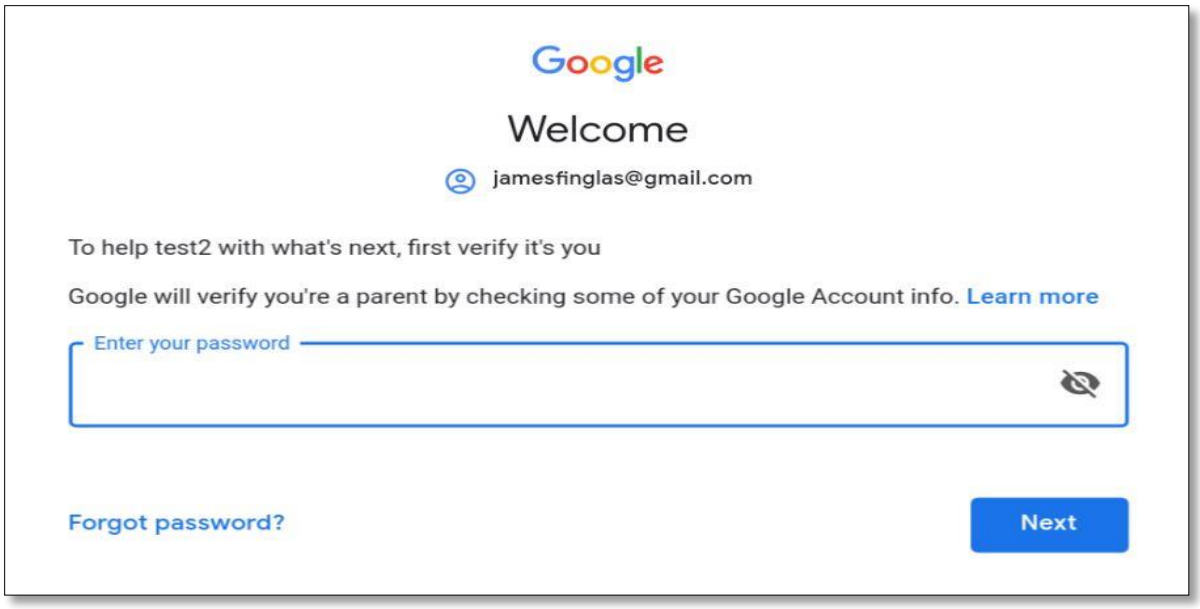


Figure 166 Enter your Google accounts password.

If two step verification is set up on the parents account, they will yet again be sent a verification code to confirm they are in fact the owner of the account.

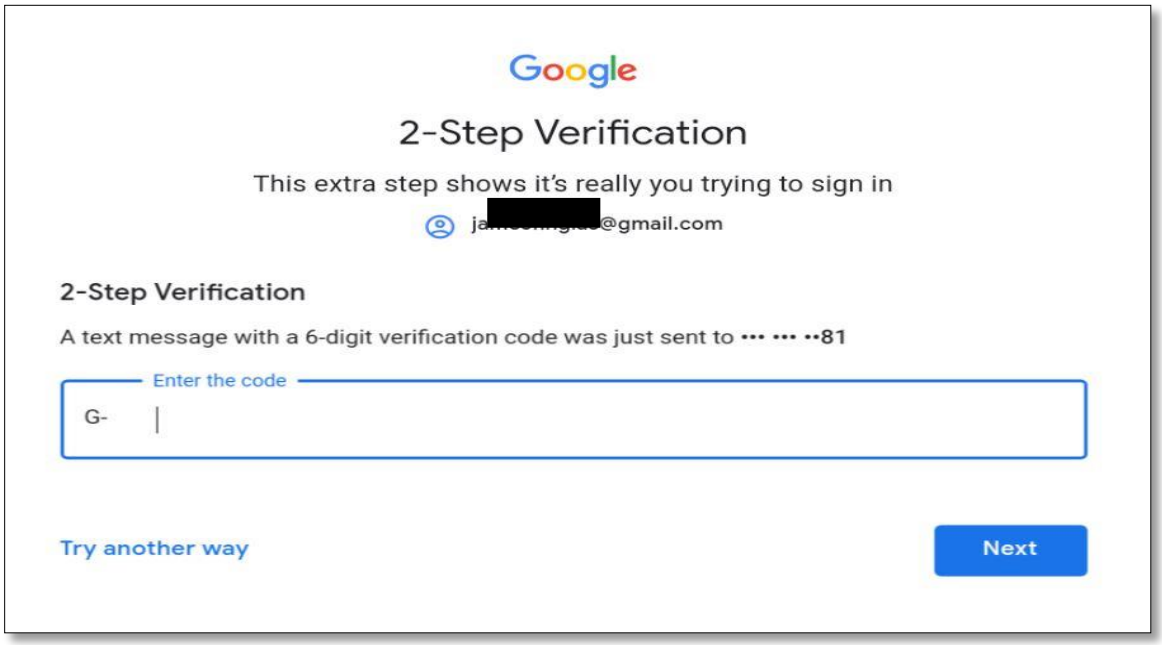


Figure 167 Enter two step verification code if required.

Next, will be presented with a brief over view of the account management options presented in Google Family-Link, once the App is installed. These include:

- The ability to choose settings and passwords
- Select the Apps your child can use and for how long (screen management)
- Set device daily use limits
- Remotely lock the device as required
- Track device locations
- Label important locations
- Approve Apps, and remove those deemed inappropriate remotely

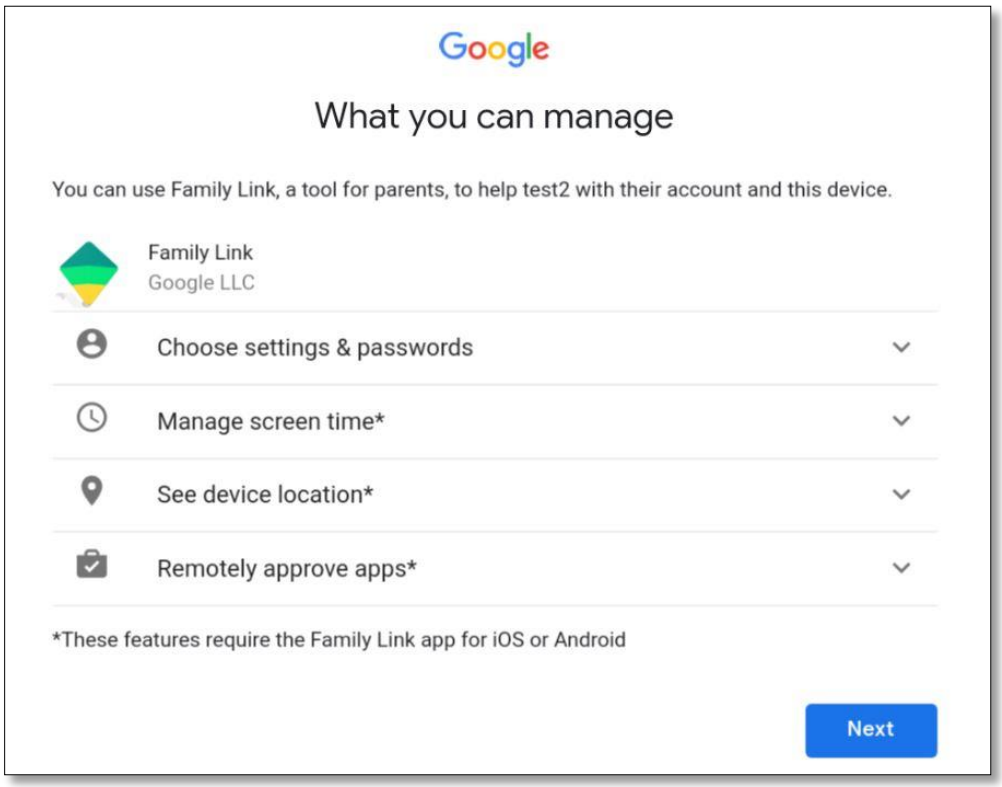


Figure 168 Overview of some of the options available.

Now we must add the child's account to our "Family" group so that we may manage their account as needed.

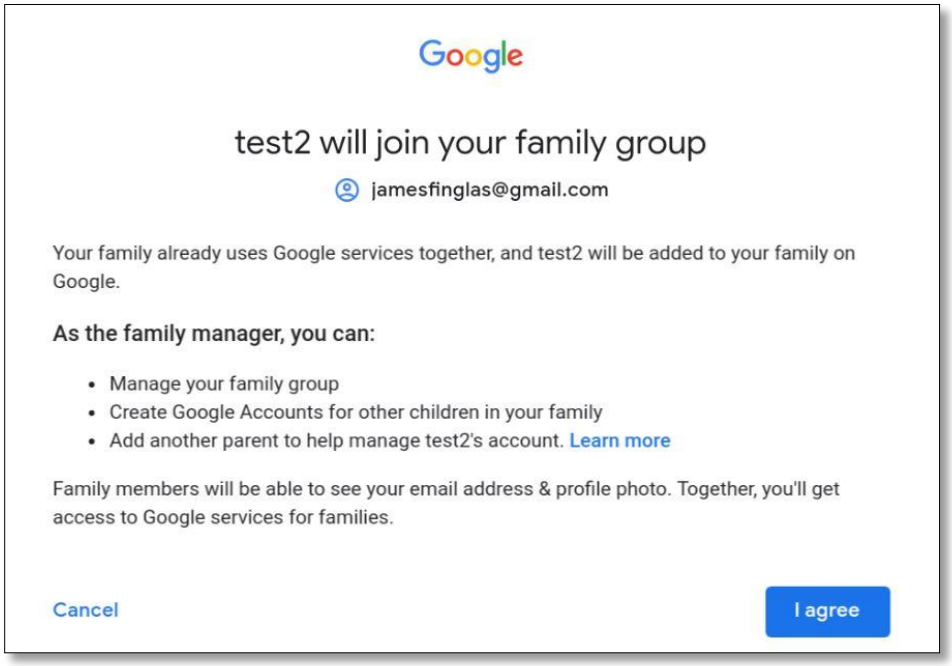


Figure 169 Select "I Agree" to add your child's account to your family group.

Next, we are presented with a significant amount of legal information relating to account privacy, data sharing and so on. Much of which was covered in Googles terms & conditions above.

Google

Parental consent

Family Link Disclosure for Parents

Welcome Parents! At Google, your trust is a priority for us and we know that allowing your child to have their own Google Account can be a big decision. This Family Link Disclosure for Parents ("Disclosure") provides important information you should consider when deciding whether to unlock the doors to the broad ecosystem of Google services. For example, we explain our data collection and use practices for your child's Google Account in the Privacy Notice for Google Accounts Managed with Family Link section below. Once you create your child's Google Account, it will be added to your family on Google and you'll be able to use Family Link's tools to help you manage the account.

In order to create a Google Account for your child, you must review this Disclosure (including the Privacy Notice below) and the Google Privacy Policy (https://www.google.com/policies/privacy/), and provide consent. Google will not knowingly collect, use or disclose your child's personal information unless you've provided this consent. We will ask for your consent before we make any material changes to the practices described in this Disclosure (including the Privacy Notice).

Figure 170 This is acknowledgement of the data protection policies and sharing employed by google. By accepting you are consenting to have Google manage your child's data and account.

Your Child's Google Account

Keep in mind that your child's Google Account will be like your own and offers access to many of Google's products and services, including general audience services that you may use yourself, such as Chrome, Search, Gmail, Google Play, Hangouts, Google Assistant, and YouTube (ages 13+ only). Most of these products and services have not been designed or tailored for children, and your child may use them to communicate with others or to find content that you consider inappropriate.

Your child will be able to use their account to do things like:

- Access and search the internet;
- Send and receive emails, chat messages, video and voice calls;
- Subject to the Google Play approval settings for their account, purchase and download apps and games, music, movies, books, and other content available on Google Play, as well as make in-app purchases; and
- Create, view, share, and receive content, including photos, videos, audio, notes, presentations, documents, and more, some of which may be shared publicly.

As explained in the Privacy Notice for Google Accounts Managed with Family Link (https://families.google.com/familylink/privacy/child-policy/) below, Google will not serve personalized ads (https://support.google.com/ads/answer/2662856) to your child, but your child will still see ads

Figure 171 Here google outline the function available which a parent may wish to secure via Family-Link, such as browser searching, emails, chats, video and voice calls etc.

Tools for Parents

Family Link

After you create your child's account, you can use Family Link to help you do things like:

- Approve your child's downloads and purchases from Google Play and limit the visibility of content in the Google Play Store based on maturity ratings;
- Manage settings such as SafeSearch for Google Search;
- Review your child's app permissions on Android, such as microphone, camera, location, and contacts access;
- Change the content filtering setting and turn search on or off in the YouTube Kids app;
- Reset your child's Google Account password;
- Set screen time limits on your child's Android devices;
- See the location of your child's signed-in and active Android devices;
- Manage the activity settings for your child's Google Account; and
- Allow a second family member to exercise most of the same controls you have over your child's account.

Figure 172 Once again, a slightly more verbose overview of the functions available in Family-Link.

These tools can help you set digital ground rules for your family. Some Family Link settings are modifiable on the web (https://families.google.com/), but you'll need the Family Link app to access the full set of tools. For example, you must download the Family Link app to use features for your child's Android device like screen time limits or app activity. Please keep in mind these tools have limitations and may require certain settings or circumstances in order to work. For example, you won't be able to see your child's device location in the Family Link app, unless the device is on, connected to the internet, and recently active. Additionally, filters like SafeSearch and Chrome website restrictions are not perfect, so explicit, graphic, or other content you may not want your child to see makes it through sometimes.

Figure 173 This simply outlines that the Family-Link App is required to access all the functions offered by Family-Link.

Google Play Parental Controls & Purchase Approvals

Your child will be able to browse a wide variety of content in the Google Play Store, including titles for apps, movies, books, and music. You should review and adjust your child's Google Play settings based on what you think is right for them. Keep in mind, these settings depend on maturity ratings provided by third parties that can be incomplete or improperly assigned, so your child may still see listings for content that you consider inappropriate regardless of the settings you choose.

By default, you must review and approve your child's purchases and downloads. Your child may request content that is designed or intended for more mature audiences, or share information and communicate with others using third-party apps installed on their device, so you should use your discretion when deciding what to approve. For example, they can share photos or videos through third-party apps. Regardless of the approval settings you choose for your child's purchases and downloads, you won't be asked to provide approval in some instances, such as if your child: re-downloads an app or other content; installs an update to an app (even an update that adds content or asks for additional data or permissions); or downloads shared content from your Google Play Family Library.

You can block apps so that they are no longer accessible on your child's Android device by tapping the "Apps" card in Family Link, selecting the app you want to block and toggling "Allow App" to off. The App will then be hidden, but not deleted from your child's device, unless you unblock it. If you delete or uninstall an app from your child's device, your child will be able to reinstall it without additional approval. You can also use Family Link to review the app permissions for your child's apps.

Figure 174 This section outlines the purchasing and approval polices by Google under Family-Link. By default, the parent must approve all purchases.

Privacy Notice for Google Accounts Managed with Family Link ("Privacy Notice")

We know it's important for you to understand what personal information we collect in association with the Google Account you create for your child, why we collect it, and how you can update, manage, export, and delete that information. This Privacy Notice and the Google Privacy Policy (https://www.google.com/policies/privacy/) explain our privacy practices for your child's Google Account. To the extent there are terms that conflict, such as with respect to limitations on personalized advertising, this Privacy Notice controls.

This Privacy Notice does not apply to the practices of any third party (non-Google) apps, actions or websites that your child may use. You should review the applicable terms and policies for third party apps, actions, and sites to determine their appropriateness for your child, including their data collection and use practices.

Information We Collect

The Google Privacy Policy (https://policies.google.com/privacy#infocollect) sets forth our information collection practices. For example, we collect:

Information you and your child create or provide to us
For example, when you create a Google Account for your child, we'll ask for personal information about them, like their first and last name, email address, and birthdate. We also collect the content your child creates, upload, or receives from others when using our services, like when your child sends or receives an email, saves a picture or video in Google Photos, or creates a document in Google Drive.

Figure 175 Privacy information continued, as well beginning to document data collection policy.

Information we get from your child's use of our services

We automatically collect and store certain information about the services your child uses and how your child uses them, like when your child enters a query in Google Search, talks to the Google Assistant, or watches a video on YouTube Kids. This information includes:

- **Your child's apps, browsers & devices**
  We collect information about the apps, browsers, and devices your child uses to access Google services, including unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your child's apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your child's request. We collect this information when a Google service on your child's device contacts our servers, for example, when they install an app from the Play Store.

Figure 176 Information regarding the collection of data from a child's online activity.

- **Your child's activity**
  We collect information about your child's activity in our services, which we use to do things like recommend apps they might like on Google Play. Your child's activity information that we collect may include things like search terms, videos they watch, voice and audio information when they use audio features, people with whom they communicate or share content, and Chrome browsing history they've synced with their Google Account. If your child uses our services to make and receive calls or send and receive messages, for example by using Google Hangouts, we may collect telephony log information like their phone number, calling-party number, receiving-party number, forwarding numbers, time and date of calls and messages, duration of calls, routing information, and types of calls. Your child can visit their Google Account to find and manage activity information that's saved in their account and you can also manage their activity information by signing in to your child's Google Account.

- **Your child's location information**
  We collect information about your child's location when they use our services. Your child's location can be determined by using GPS, IP address, sensor data from their device, and information about things near their device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices. The types of location data we collect depends in part on your child's device and account settings.

- **Your child's voice & audio information**
  We may collect your child's voice and audio information. For example, if your child uses audio activation commands (e.g., "OK, Google" or touching the microphone icon), a recording of the following speech/audio, plus a few seconds before, will be stored to their account from any of your child's signed-in devices, when the Voice & Audio Activity setting is enabled.

Figure 177 Information regarding the collection of data from your child's in App activity, voice and video data and location data.

We use various technologies to collect and store your child's information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

We do not require your child to provide more personal information than is reasonably necessary to use the Google products and services available for these accounts.

How We Use Information We Collect

Google's Privacy Policy explains in greater detail the purposes for which Google collects data (https://policies.google.com/privacy#infouse) in association with your child's Google Account. In general, we use your child's information to provide, maintain, and improve our services; to develop new services; to customize our services for your child; to measure performance and understand how our services are used; to communicate directly with your child in relation to our services; and to help improve the safety and reliability of our services.

We use different technologies to process your child's information for these purposes. We use automated systems that analyze your child's content to provide them with things like customized search results or other features tailored to how they use our services. And we analyze your child's content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable their account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

We may use your child's information to provide recommendations, personalized content, and customized search results. For example, depending on your child's settings, Google Play may use information, like apps your child has installed, to suggest new apps they might like.

In addition, we may combine the information we collect among our services and across your child's devices for the purposes described above. Depending on your child's account settings, their activity on other sites and apps may be associated with their personal information in order to improve Google's services.

Google will not serve personalized ads (https://support.google.com/ads/answer/2662856) to your child, which means ads will not be based on information from your child's account. Instead, ads may be based on information like the content of the website or app your child is viewing, the current search query, or general location (such as city or state). When browsing the web or using non-Google apps, your child may encounter ads served by other (non-Google) ad providers, including ads personalized by third parties.

Information Your Child Can Share

Your child will be able to share information, including photos, videos, audio, and location, publicly and with others, when signed in with their Google Account. When your child shares information publicly, it may be accessible through search engines like Google Search.

Information Google Shares

Information we collect may be shared outside of Google in limited circumstances. We do not share personal information with companies, organizations, and individuals outside of Google except in the following cases:

With consent
We will share personal information with companies, organizations or individuals outside of Google with consent (as applicable).

Figure 178 Information regarding how data is collected, and on what kinds of data your child can share both with and without consent.

With your family group
Your child's information, including their name, photo, email address, and Play purchases, may be shared with members of your family group on Google.

For external processing
We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with this Privacy Notice, the Google Privacy Policy (https://policies.google.com/privacy), and any other appropriate confidentiality and security measures.

For legal reasons
We will share personal information outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- meet any applicable law, regulation, legal process or enforceable governmental request;
- enforce applicable Terms of Service, including investigation of potential violations;
- detect, prevent, or otherwise address fraud, security or technical issues; or
- protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

Figure 179 Information regarding the visibility of your child's account regardless of how restrictive your settings are.

We may also share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from browsers or devices for advertising and measurement purposes using their own cookies or similar technologies.

If your child is signed into YouTube Kids with their Google Account, this Privacy Notice applies. If your child is not signed into YouTube Kids with their Google Account, the YouTube Kids Privacy Notice applies.

Figure 180 Information regarding the sharing of data between YouTube and its partners.

Access to Your Child's Personal Information

As a parent, you can access, update, remove and export your child's information by signing into their Google Account. If you do not remember your child's password, you can reset it through the Family Link app or Family Link settings on the web (https://families.google.com/). Once signed in, you can use the various controls described in the Google Privacy Policy (https://policies.google.com/privacy#infochoices) (such as Google activity controls (https://myaccount.google.com/activitycontrols)) to manage your child's privacy settings and information. Your child will have the ability to change their activity controls, delete their past activity in "My Activity," and grant app permissions (including things like device location, microphone, or contacts) to third parties. However, you can limit your child's ability to change their activity controls without parental approval by going to Family Link settings (either in the app or on the web) and changing their "Manage Google Activity" settings to "Only parents." If your child's device is running Android 6.0 or higher, you can also change their "App Permissions" settings to "Only parents."

You can also use the Family Link app or Family Link settings on the web to edit or modify your child's Google Account information, review app activity and app permissions, and, if your child's device is running Android 6.0 or higher, manage your child's ability to grant certain permissions to apps to do things like access information from your child's Android device (such as location, microphone, and contacts). You can also use Family Link to help manage your child's access to certain features, apps, and services on Android.

Figure 181 Information regarding who can access your child's personal information.

If at any time you wish to stop further collection or use of your child's information, you can delete your child's Google Account my clicking "Delete account" on your child's Account Info page in Family Link or on the Family group page in My Account (https://myaccount.google.com/family). Your child's account information will be permanently deleted within a reasonable period of time.

Figure 182 Information regarding the deleting of your child's account and how it will stop the collection of data.

When Your Child Can Manage Their Account on Their Own

When your child turns 13 (or the relevant age as determined by applicable law in your jurisdiction) (https://support.google.com/accounts/answer/1350409?p=families_aoc&visit_id=1-636616671949049601-3410216769&rd=1&), they are eligible to manage their account on their own. If your child chooses to manage their Google Account, you will no longer have access to, or be able to exercise control over it, with Family Link. Before your child becomes eligible to manage their own Google Account, we will notify you and your child.

Figure 183 Once your child turns 13, because they can technically manage their own account from this point on. The child can take over the account without the parent's approval at this point despite the digital age of consent in Ireland.

Contact Us

If you have any questions about your child's Google Account, don't hesitate to contact us. We're here to help. You can find additional information about Family Link and your child's Google Account in our help center (https://support.google.com/families?p=parentalconsent_help). You can also send us feedback about Family Link or your child's Google Account in the Family Link app by tapping Menu ☰ > Help & Feedback > Send feedback, or by contacting us by email (https://support.google.com/families/contact/families_email?hl=en&cfsi=families_support&cfnti=escalationflow.email&cft=3) or at the address below.

Google
1600 Amphitheatre Parkway
Mountain View, CA 94043 USA
Phone: +1 855 696 1131 (USA)
For other countries, visit g.co/ContactFamilyLinkHelp (https://g.co/contactfamilylinkhelp)

If you have questions about how Google collects and uses your child's data, you can contact Google and our data protection office (https://support.google.com/policies/troubleshooter/7575787). You can also contact your local data protection authority if you have concerns regarding your rights under local law.

Figure 184 Contact information for Google US, however Google is managed in Ireland by Googled Ireland LLC.

As described above, we collect information directly from you and your child, such as names and email addresses, and collect information related to your child's use of our services, such as device information, log information, voice & audio information, and location information. As explained in the section entitled "Information Google Shares" above, this information may be shared outside of Google in limited circumstances. Your child may also create and share data publicly through their use of the services. We use cookies and similar technologies to provide Google's services. We combine data among our services and across your child's devices for various purposes, including to deliver more personalized content, improve the quality of our services and develop new ones, improve security, and conduct analytics and measurement to understand how our services are used. We may use contextual information, such as a current search query or the content of a website your child is viewing, to show ads. We don't use information in your child's account to personalize ads they may see. We explain our data collection and use practices for your child's Google Account in more detail, and provide more information about the controls available to you and your child, in the Privacy Notice for Google Accounts Managed with Family Link.

Please agree to continue:

☐ I agree to let Google create a Google Account for my child and process their information as described above and further detailed in the Privacy Notice for Google Accounts Managed with Family Link and the Google Privacy Policy. I am authorized to provide this consent.

☐ I understand that my child's Google Account is like my own and will provide access to general audience services that have not been designed for children and that will enable my child to do things like communicate with others and see content I may consider inappropriate. I also agree to the Google Terms of Service, the Chrome Terms of Service, the YouTube Terms of Service, and the Google Play Terms of Service on behalf of my child and understand that all terms apply to my account and to the account I create for my child.

Cancel Agree

Figure 185 Finally, the parent must accept the above terms & conditions, as previously covered.

Once you have read through all the legal information, you enter the final setup phase, and it is at this point that we can begin to establish basic rules regarding the child's account. This begins with setting up restrictions for the use of the google stores, play, movies, music, and books, as well as Google Chrome as seen below.

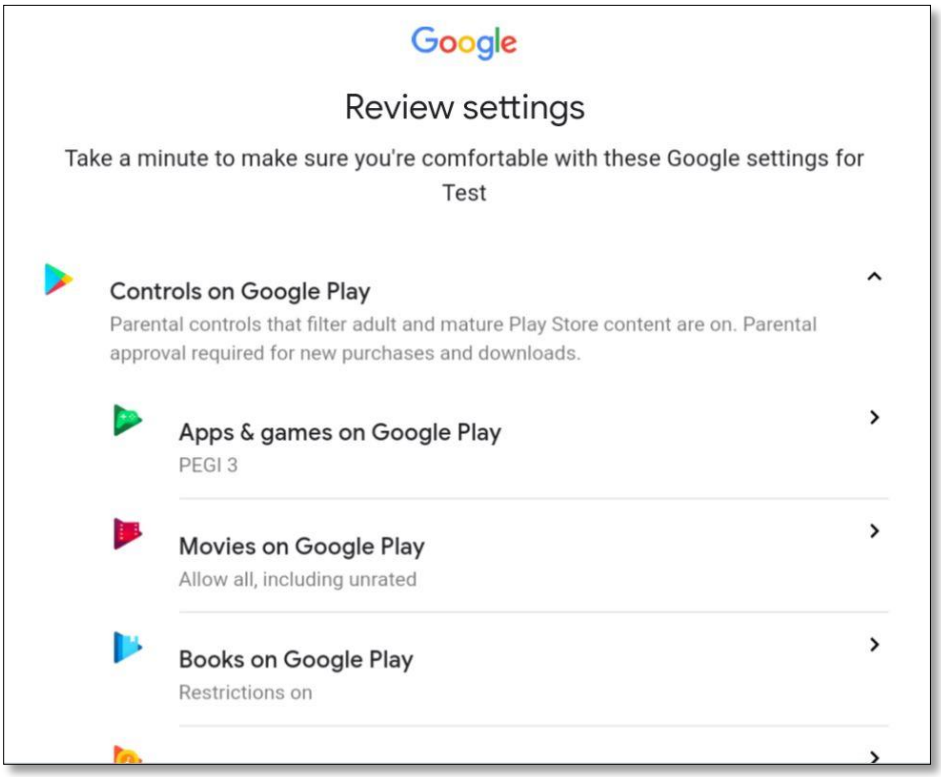


Figure 186 Here we begin to restrict the child's access to unauthorized services.

First, we will restrict the child's access to Google play games and Google movies content to age appropriate content. As seen below, we selected the most restrictive setting, however it is up to each parent to select what they feel is the appropriate setting for their child.

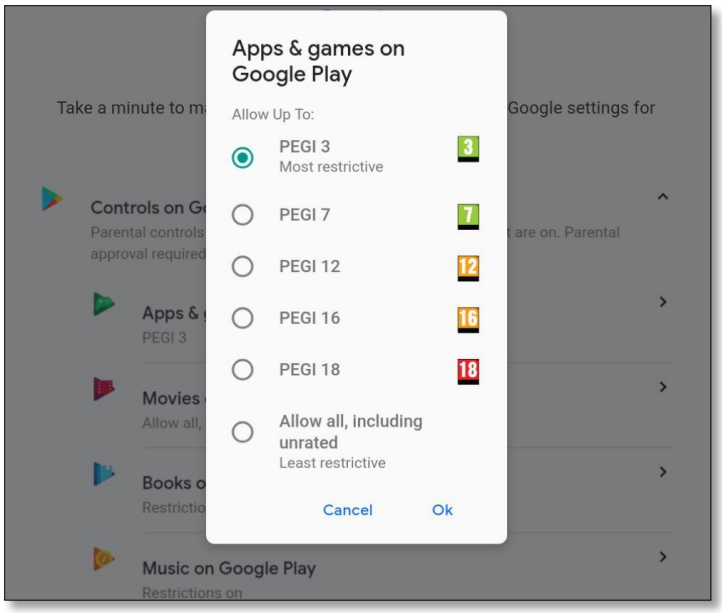


Figure 187 Select the age group of the content most appropriate for your child.

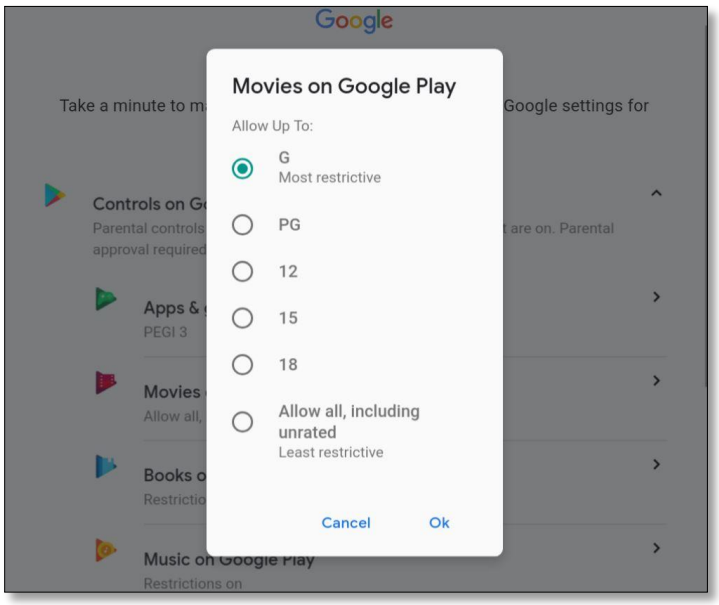


Figure 188 Select the most age appropriate movies settings.

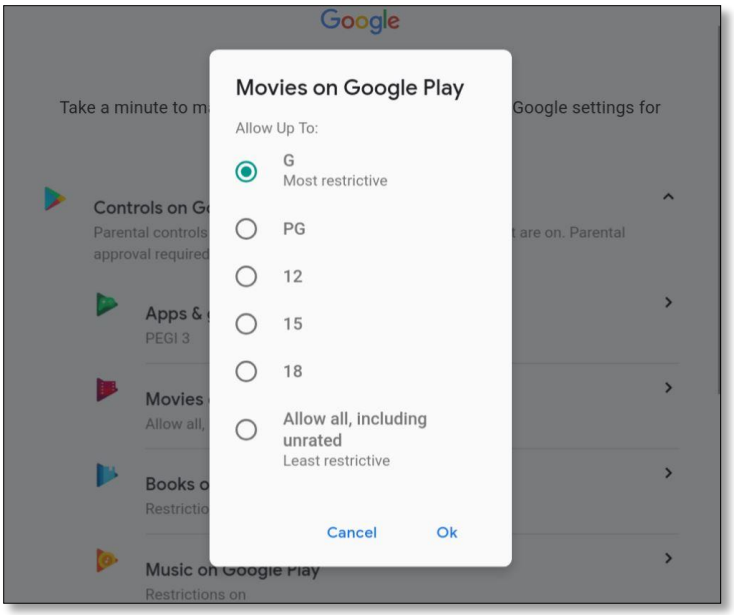


Figure 189 Select an appropriate age group for the movies your child will have access to.

Next, we check the settings of Goggle books and music, and we see that the protections are automatically applied.

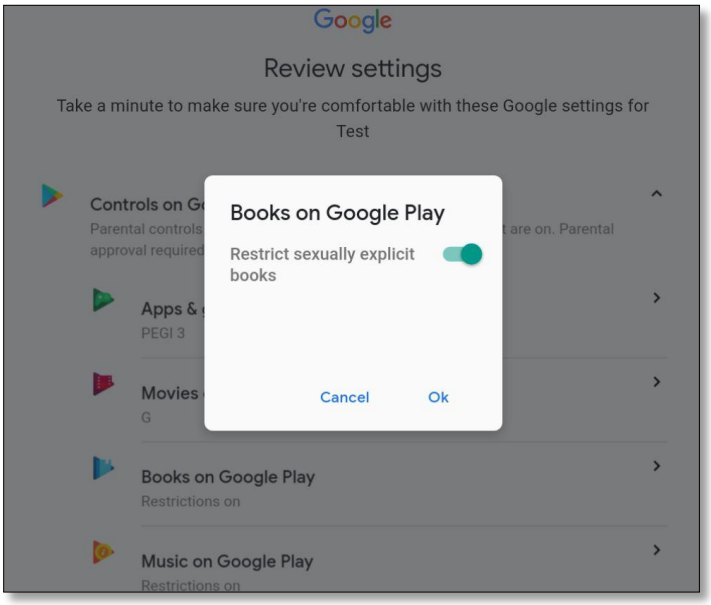


Figure 190 Here can see protections automatically applied for Google Books.

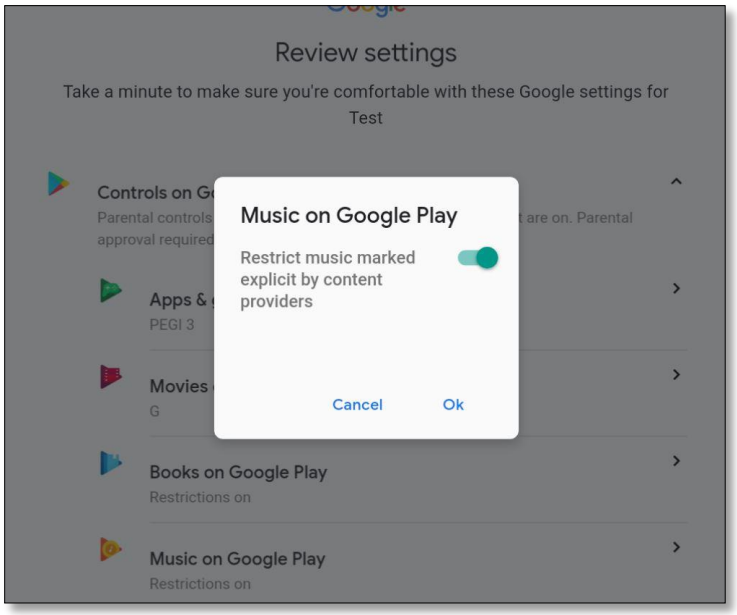


Figure 191 Again, here can see protections automatically applied for Google Music.

Next, we scroll down to see protection filters are also automatically applied to Google Chrome, which will filter out inappropriate sites which may be manually entered, and search results that may inadvertently be returned from an innocent search. However, patterns should remember these types of filter use a best guess approach and are not perfect.

We can alter these filters to be even more restrictive if required. As you can see below, we alter the filter to be at its most restrictive.

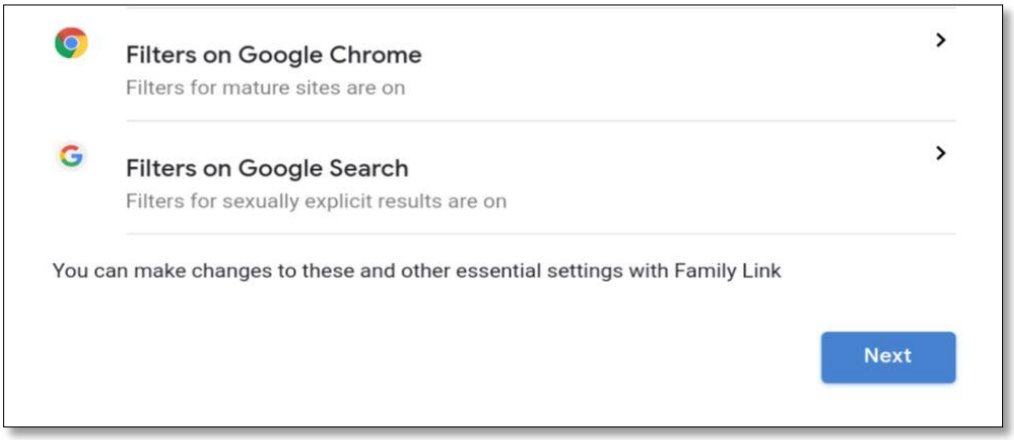


Figure 192 Here we can see filters are applied for Google Chrome browser content and search content.

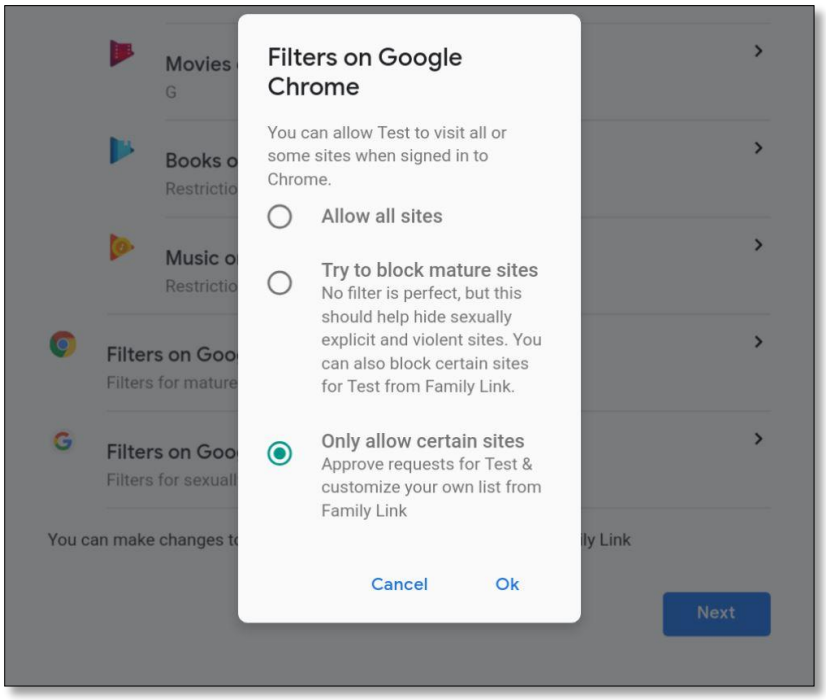


Figure 193 Here, we have increased the restrictions on google Chrome filters.

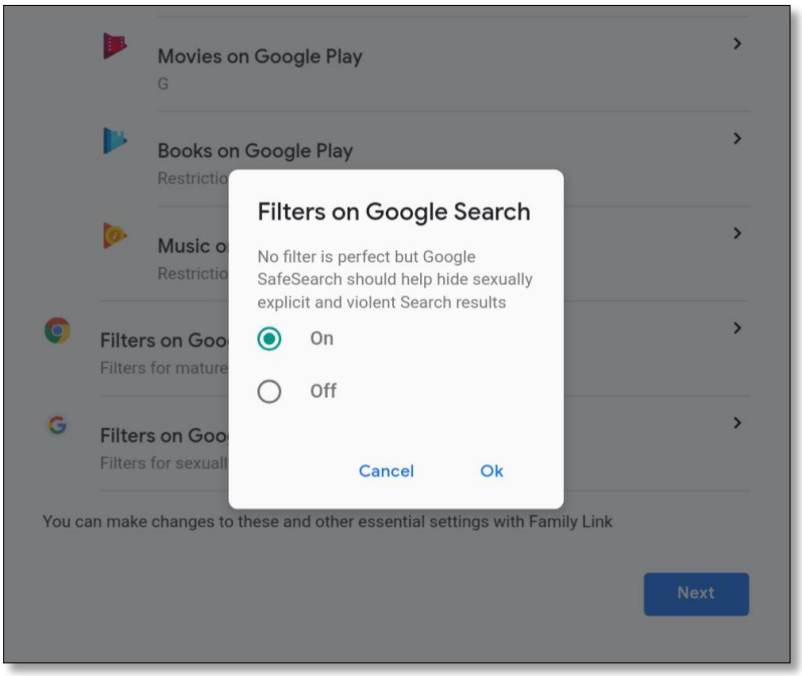


Figure 194 Here we see the safe search filters are automatically applied to Google Chrome.

Finally, we are ready to install the Family-Link App, and we are presented with a convenient option to install it during the account creation and set up phase as seen below.

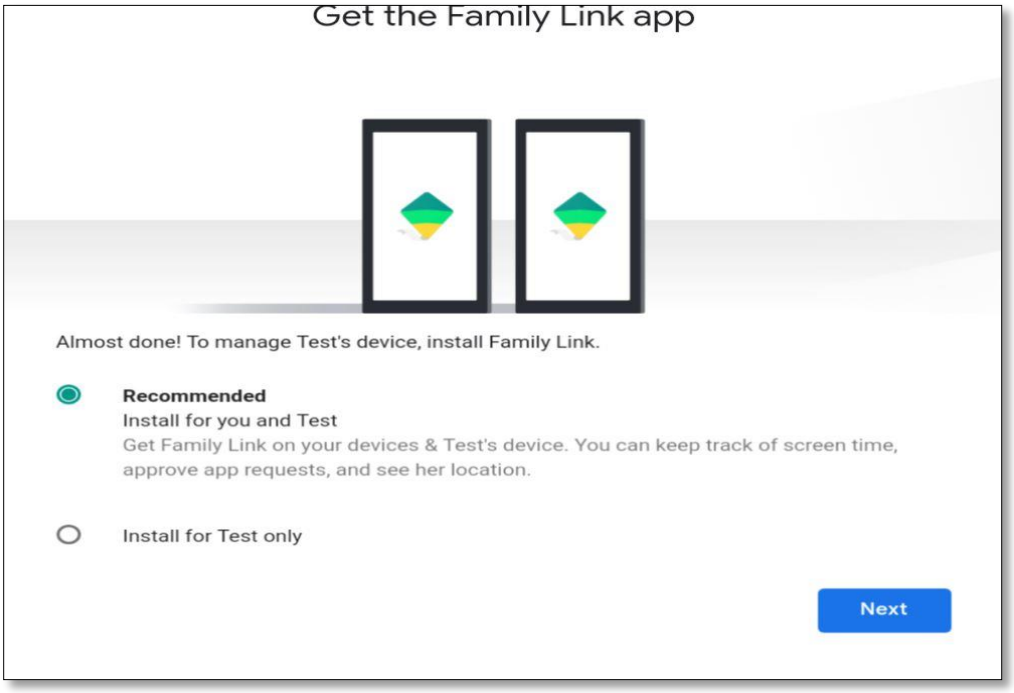


Figure 195 Now we can finally install the Family-Link App.

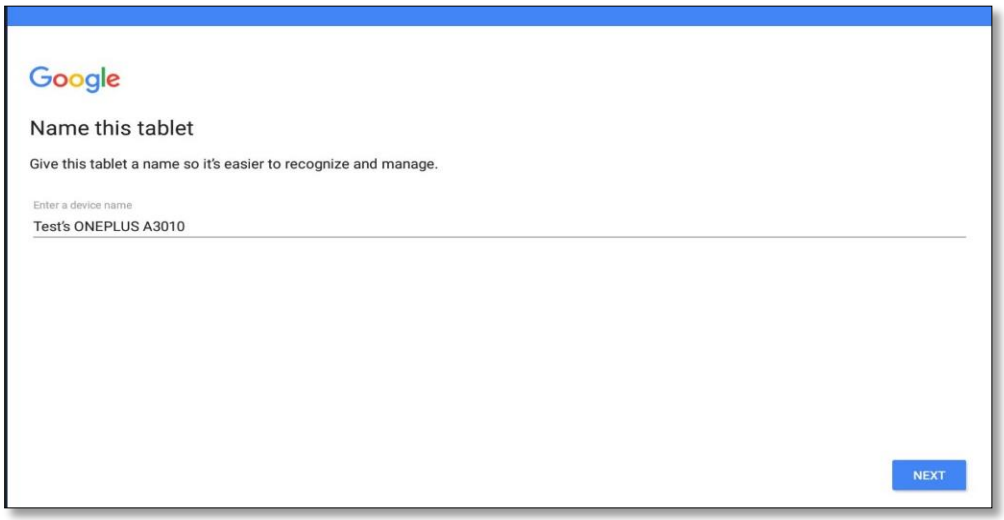


Figure 196 Here we are, installing the Family-Link App on our 'Test' child's tablet.

Having downloaded the App, once we begin installation the App will scan the pre installed Apps to see if any might be deemed inappropriate by the parent. You can select which Apps you would like to keep, or remove. During a fresh install, it is reasonable to assume they will all be safe, however, we recommend you always examine the list, just in case there are any Apps that might somehow circumevent the protections you are setting up for your child.

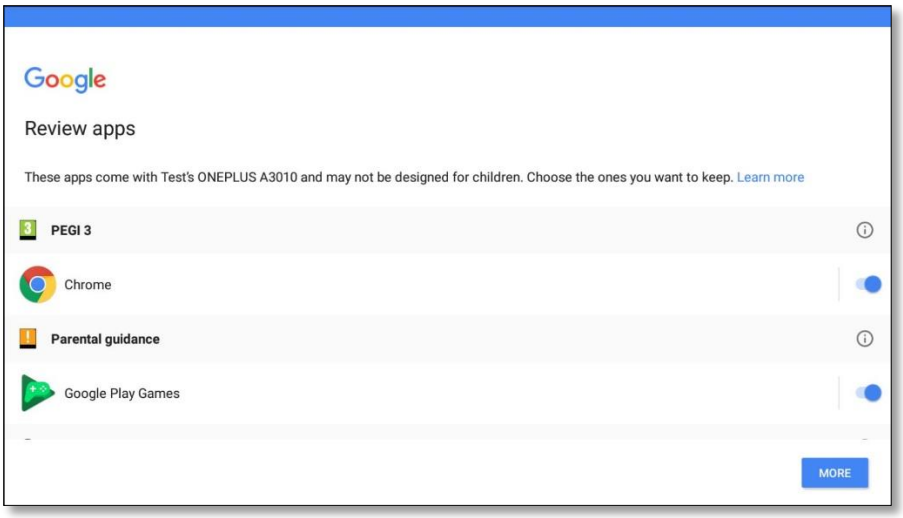


Figure 197 The App has scanned our child's tablet and presented us with a list of Apps to review and decide which would like to keep or uninstall.

Lastly, we select our backup, GPRS location data and usage data settings. Since our aim is to provide the best security possible, we recommend that back up options be disabled, as well as location data and usage options.

App updates are not configurable, and Apps will be auto updated by default. This is a good security feature, as an App is at most secure when kept up to date.

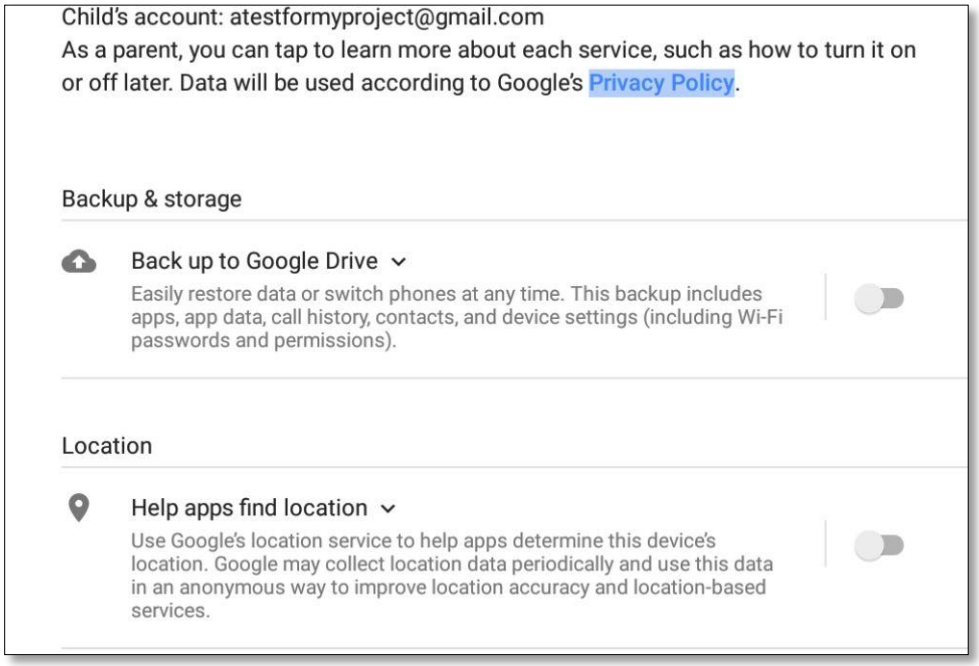


Figure 198 Here we have deactivated google bac-ups, and location data options.

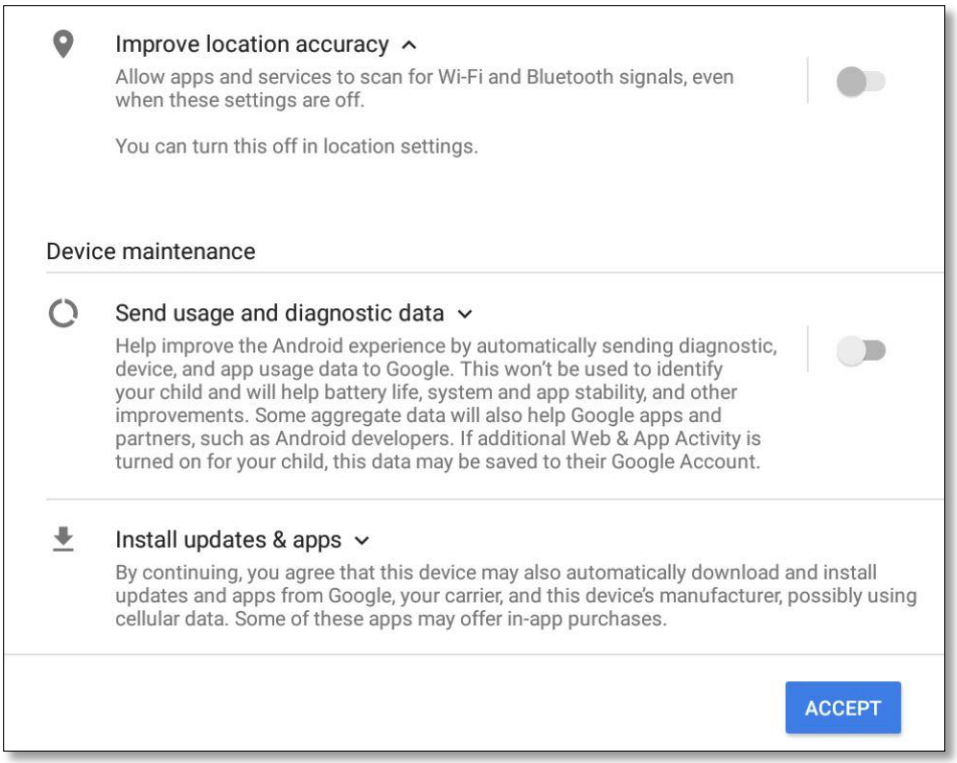


Figure 199 Lastly, we disable usage data collection. Updates cannot be disabled.

And that is it. We now have Family-Link set up on our child's device with basic initial protections set up and we are ready to begin the set up for YouTube Kids.

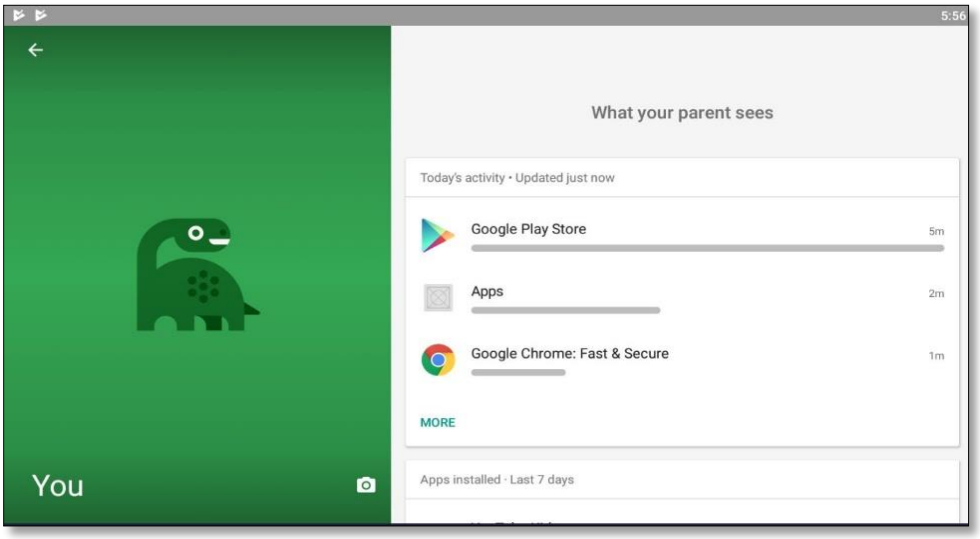


Figure 200 Here we see Family-Link set up on our "Test" child's Tablet device.

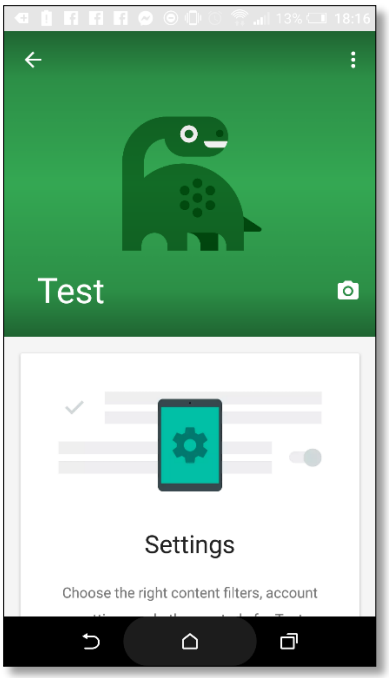


Figure 201 Here, we can see the Parent managing the "test" child's account from our group members Google account via his phone.

Now that we have our accounts set up as required, we can move on to our next stage. However, during our investigation into Family-link, we found the security features and options so good that we have elected to cover this App in detail in another section, as we feel that is in an incredibly useful security tool that any parent might wish to avail of for protection their child's device, as well as managing their child's use of their device.

11.4.2.4 Google Family-Link Settings

Parental View:

Our first step in investigating Family-Links features is examine the main screen. Here we find basic account related settings on the top left and right. Also, we can view the Accounts the parent account is currently managing. As we can see below my account is currently managing two child accounts, "TEST" and "TEST2".

At the top left denoted by the three dashes is a menu which brings us to some basic account management settings pertaining to the parent account. And on the top right, this takes us into some basic account management options for the Child account being managed.

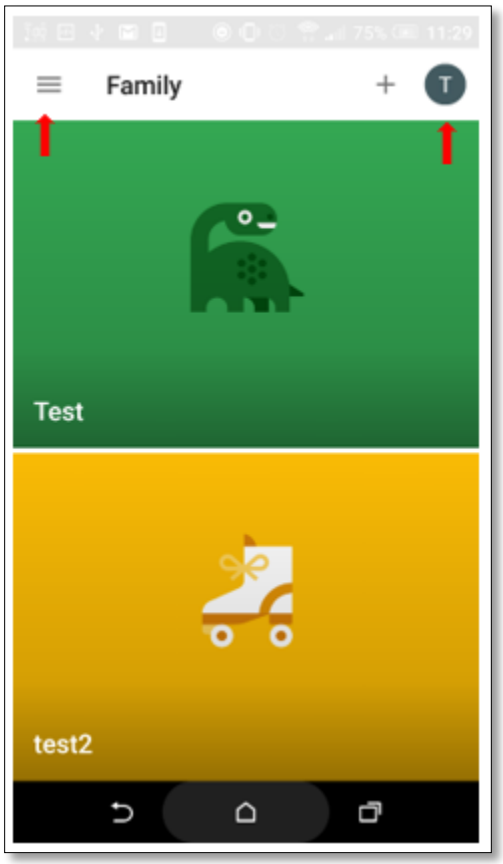


Figure 202 Here we have the main menu for Family-Link displaying all the Child accounts my account is currently managing.

Below, we can see the menu options available regarding parental account management. The first two options displayed here, “Test” and “Test2” are the accounts currently being managed and selecting either of these will take the user straight into these accounts for direct account management.

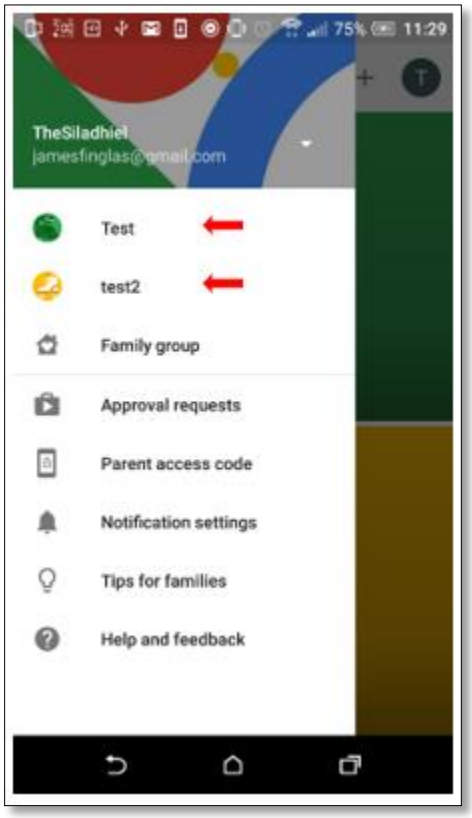


Figure 203 Here we see the test child accounts we added to our parent account.

Next up, we have the Family group menu. This menu allows us to add family members to our group. Including new parents to control our child accounts. We can then assign privileges as required.

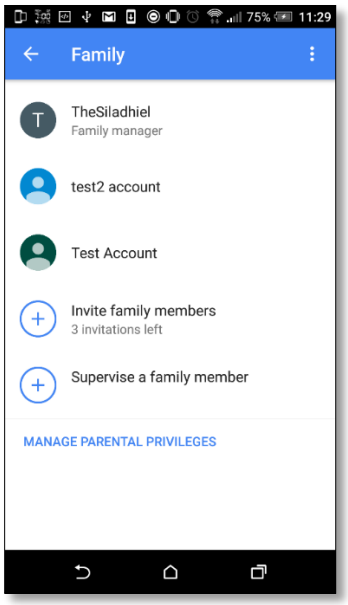


Figure 204 Here we can invite family members, assign supervisor roles and manage parental privileges as needed.

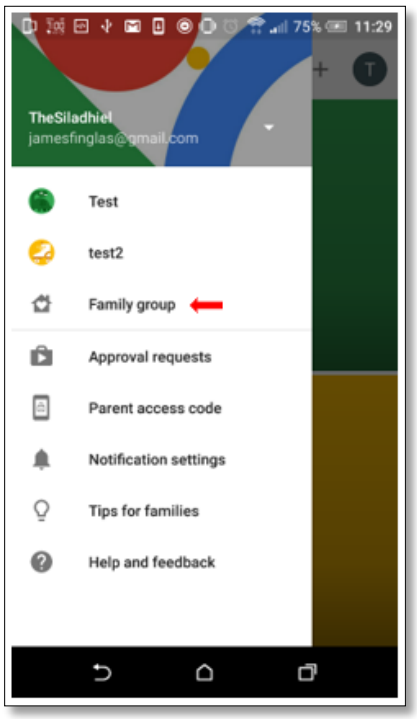


Figure 205 Here we can select the family group menu.

Next up, we have the approval requests menu. I have made a request on the “Test” child account to demonstrate this process. We first see the list of approval request messages which we can then select individually. Each request will last 24 hours before expiring.

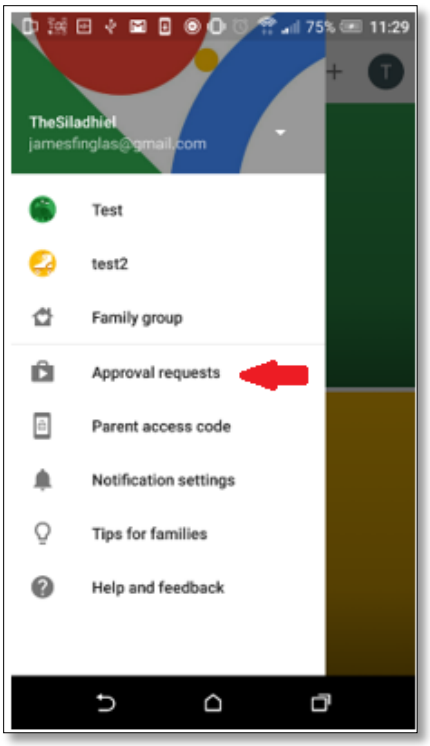


Figure 206 Select this menu to approve or deny requests.

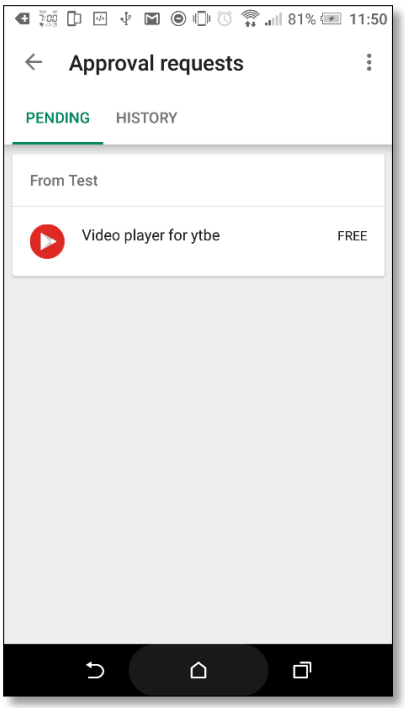


Figure 207 Here we see an approval request message has been sent from the child account.

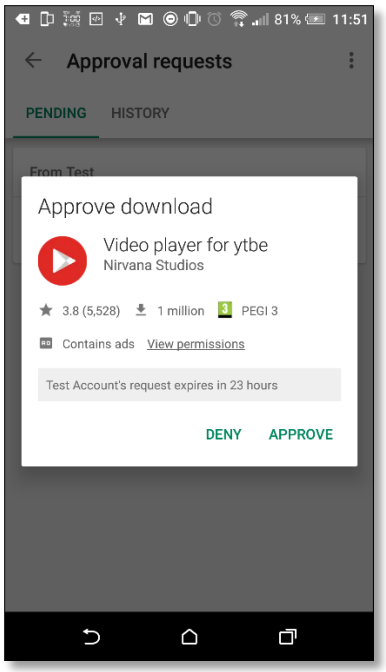


Figure 208 Here we can approve or deny the request simply be selecting the appropriate option.

For demonstration purposes, I denied this request, and below you can see how this is presented on the Childs device.

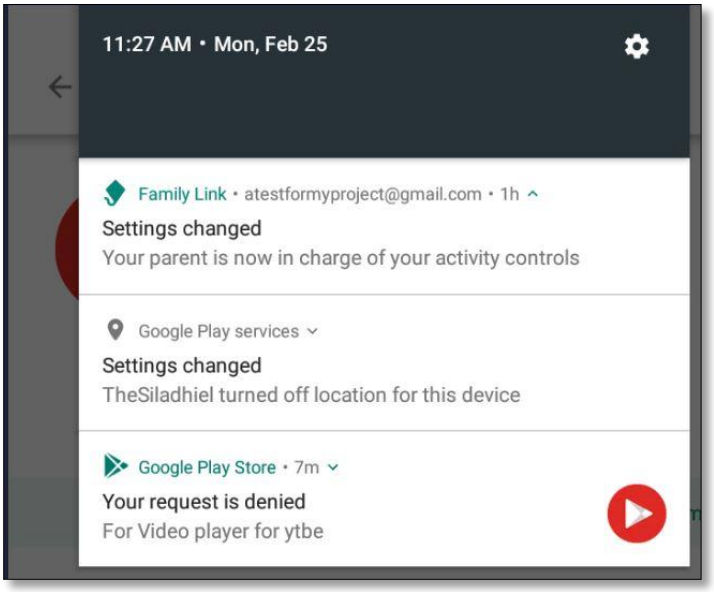


Figure 209 Here we see the request is denied on the child's device.

Following immediately after Approval settings is the parental access code. This code is used to remotely lock or unlock the child's device. This code is also needed should the parent wish to delete the child's account remotely. The code regularly changes. This is a very useful security feature provided by Google.

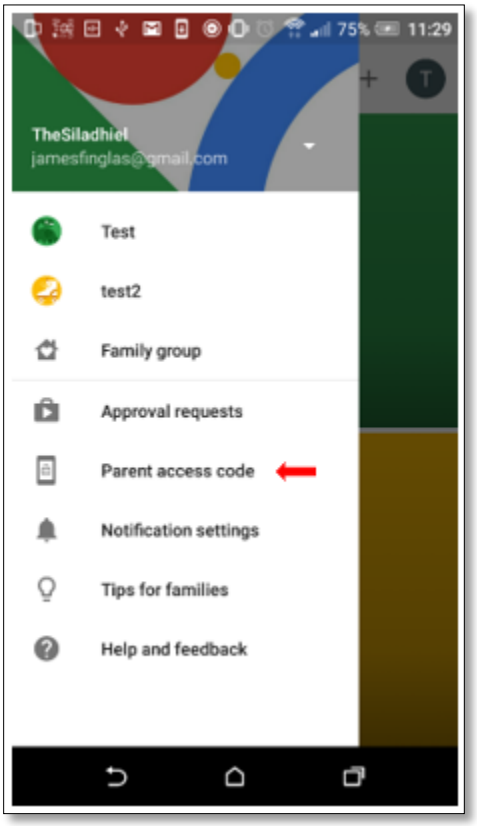


Figure 210 Here we can see the parental code menu option displayed.

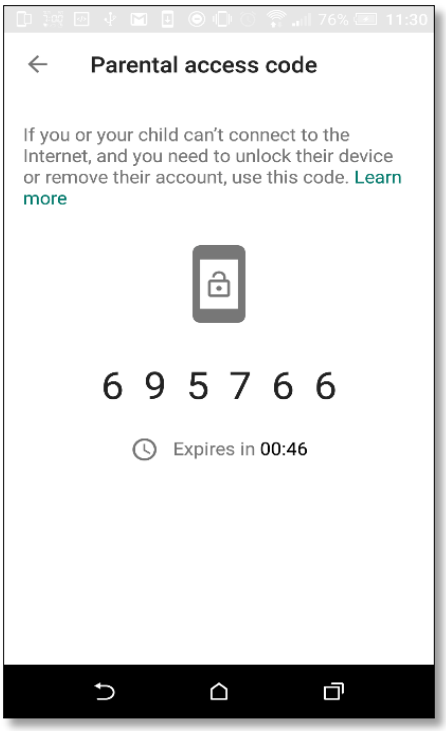


Figure 211 Here we see the parental access code. This code changes regularly as you can see by the timer above.

Next up in the parental account management section is the notification management section as seen below.

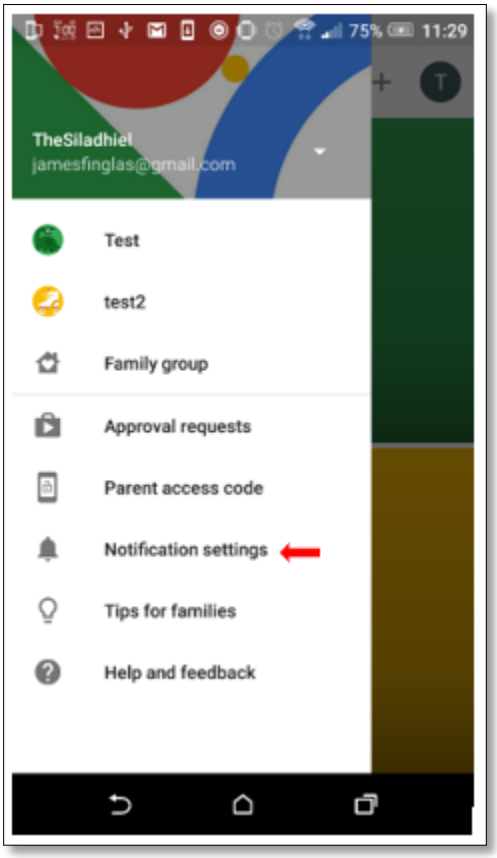


Figure 212 Here, we select the notification management settings.

These settings are import and will determine precisely what activity the parent will track on the child's device/account. You can select App notifications and E-mail notifications for when you are away from your own device and wish to check up on your child.

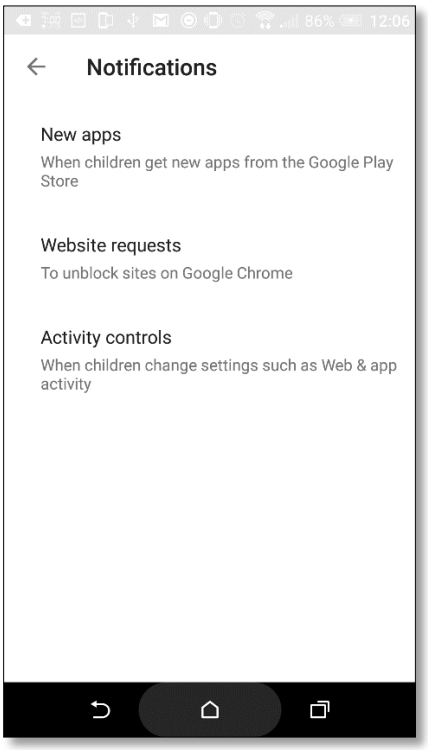


Figure 213 Here we see the available categories of notifications.

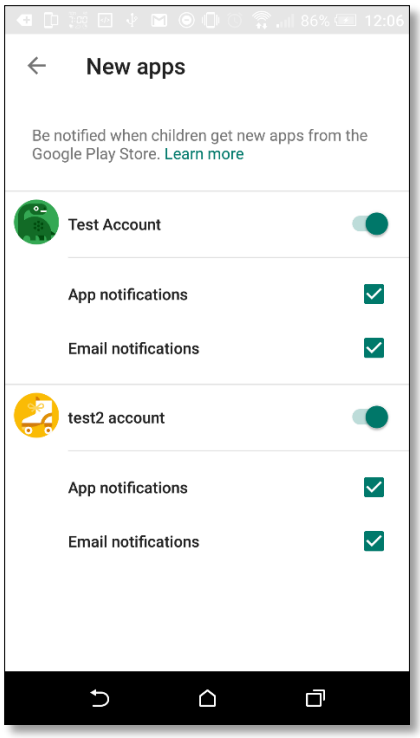


Figure 214 Here we can manage the notifications related to new Apps.

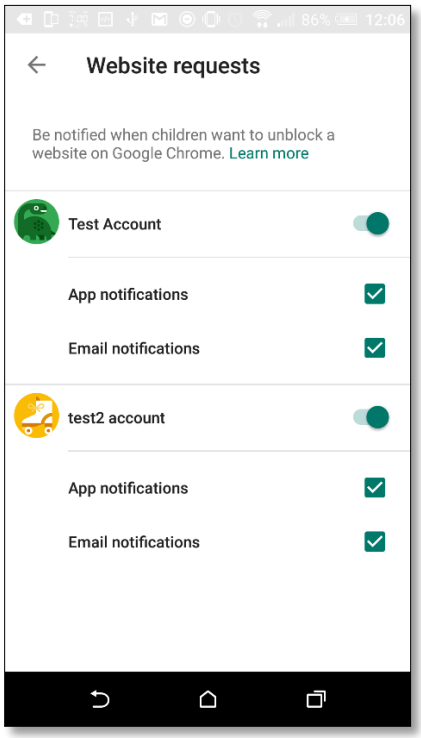


Figure 215 Here we can see the available options for Website notifications.

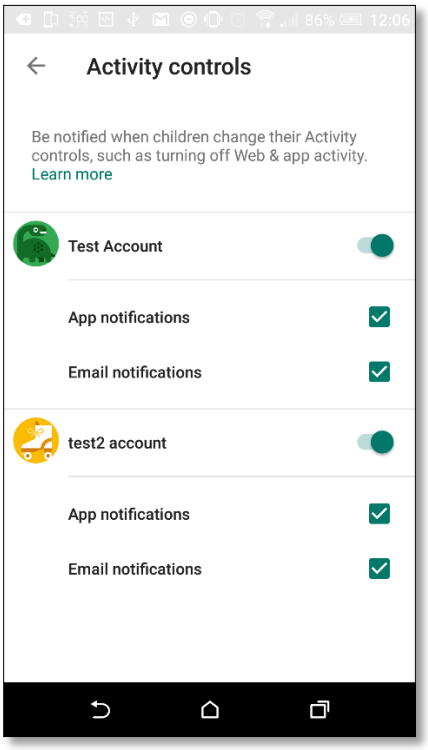


Figure 216 Here we can see the options available for Activity notifications.

The final two options offer useful tips and help options for parents. While we will not display all these options here, we do strongly recommend that user examine these tips and links as we feel that they do contain useful information for those are not quite as tech savvy as regular computers or device users may be.

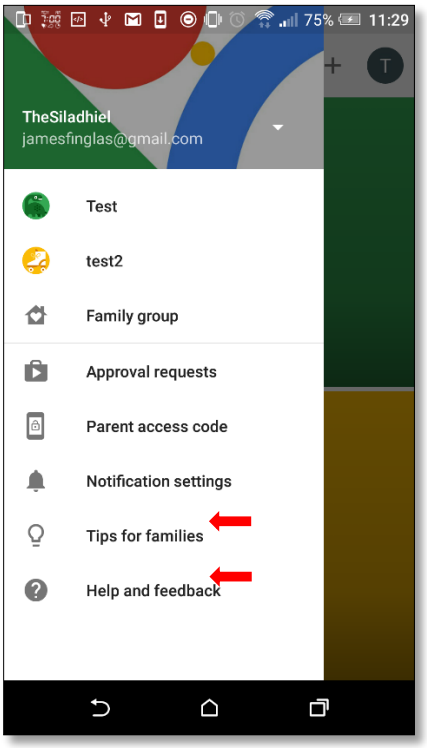


Figure 217 Here we see the tips and help/feedback menus.

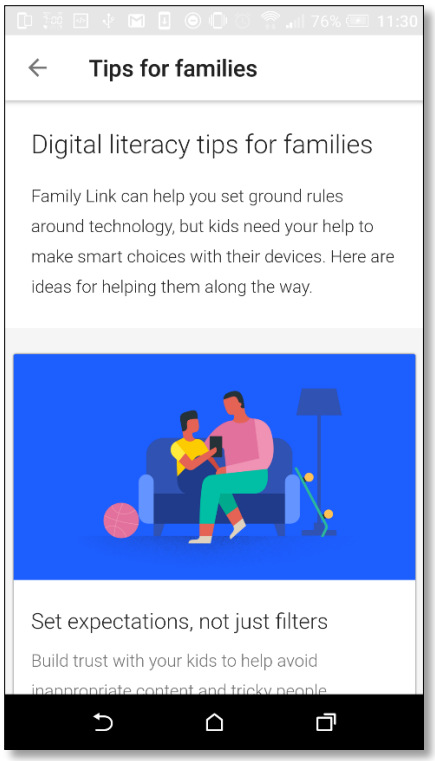


Figure 218 Here we see a sample of the tips displayed in the tip's menu. We strongly recommend parents examine these tips.

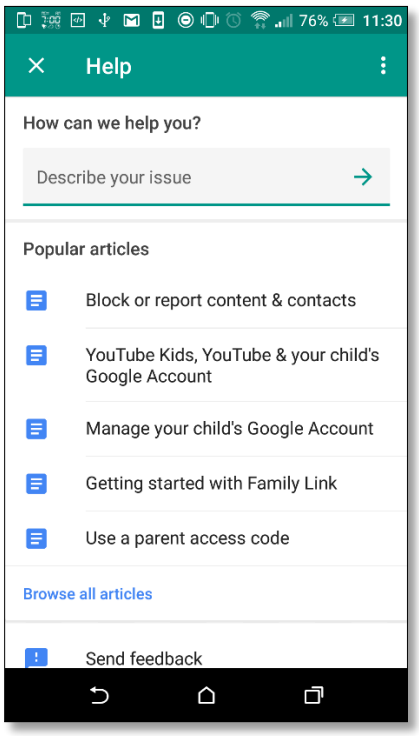


Figure 219 Here we see some of the help and feedbacks options displayed. Again, we strongly recommend parents examine this section in depth.

We will now return to the main menu to examine the main menu options previously mention on the top right of the screen. As we can see below, we have two available options. If we select the “T” option which denotes the parent account, this beings up the family group management options previously covered above. This is perhaps not adequately explained by the program. However, there is one function we will mention that we did not previously mention. This is the delete family group option. Use caution here as activating this option will of course delete your child’s account and remove your ability to manage it.

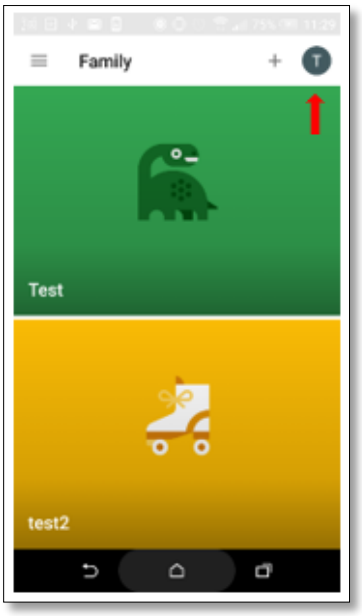


Figure 220 Here we see the options mentioned previously which give us access to other options pertaining to account management.

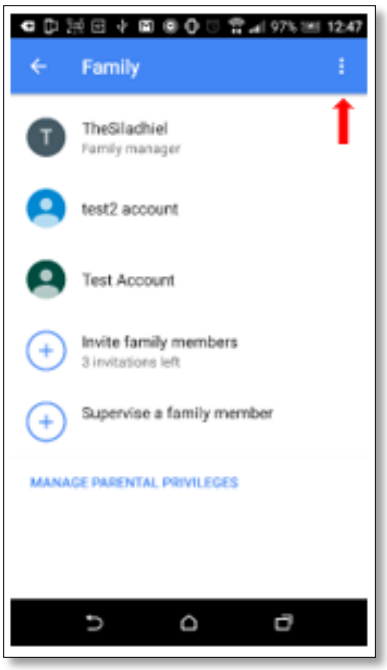


Figure 221 Here see, once again the family group options. Please note the three dots which contain the 'Delete family Group" option.

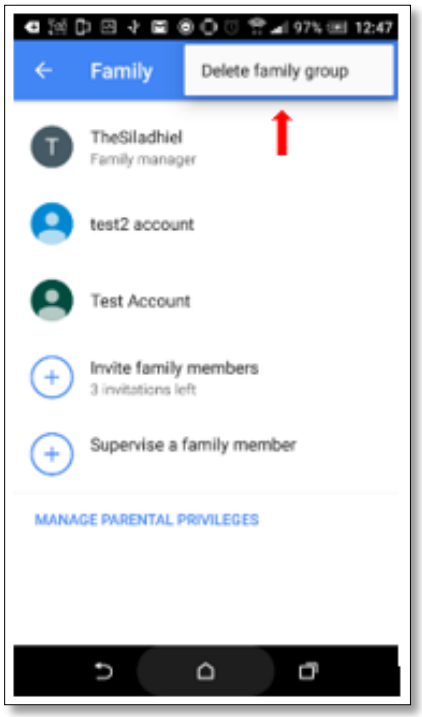


Figure 222 Here we see the delete family group option displayed, use caution as this will also remove your child's account and prevent you from managing it.

Last up in the main menu settings, we have the + icon located just beside the parent account icon. This option allows you to add accounts to Family-Link to be managed. Please note, for an account to be managed, it must first be added to your family group as shown previously.

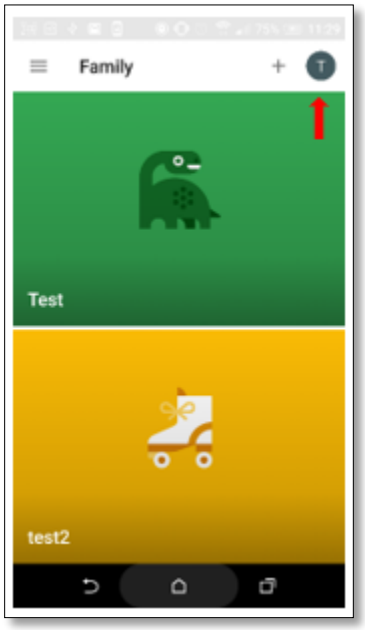


Figure 223 Here we see the + add child account option.

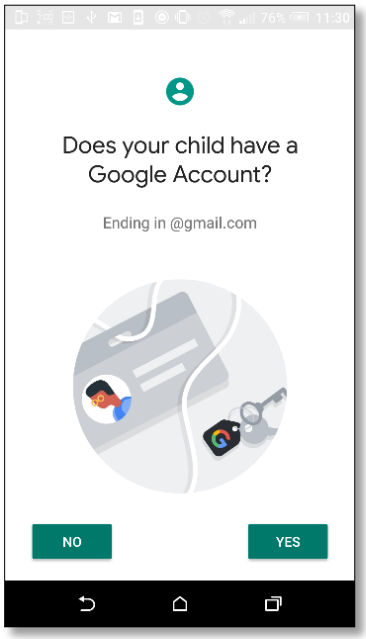


Figure 224 Here we can see that we can now add a new child account.

Now it's time to move on to direct account management of our child's account. From the main menu simply select your child's account. In this test case, I chose 'Test' as the account I wish to manage.

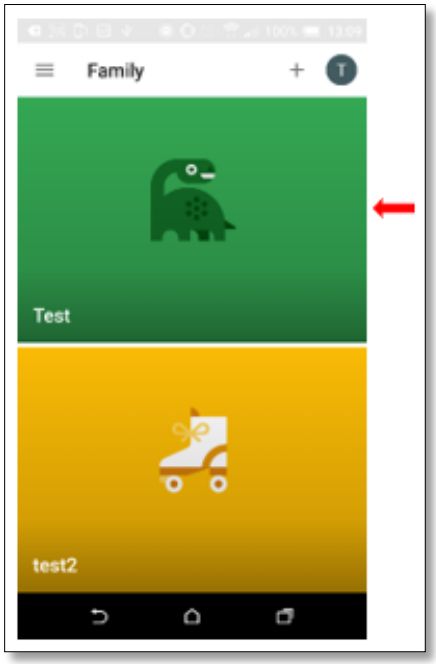


Figure 225 Here we select the account we wish to manage, in this case the "Test" account.

The first setting of note is the ability to access the account details of the account we are managing, and alter them, denoted by the three dotes on the right of the screen. This can also be accessed via another menu yet to be covered. From here the account may also be deleted if desired.

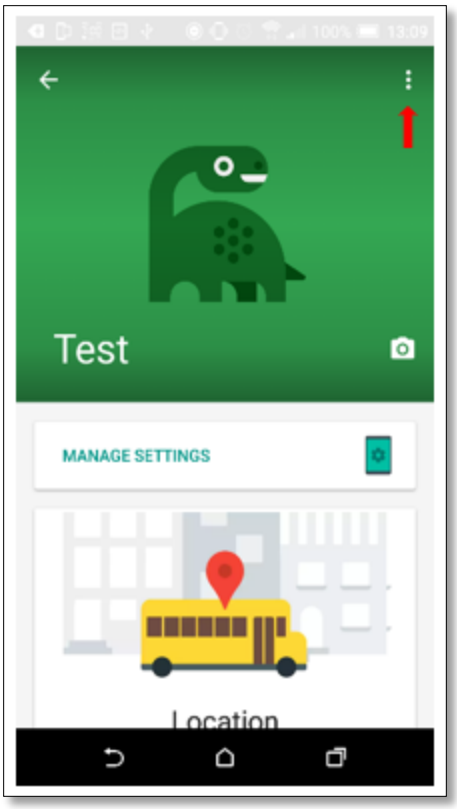


Figure 226 Here we are, in the Test account management menu screen.

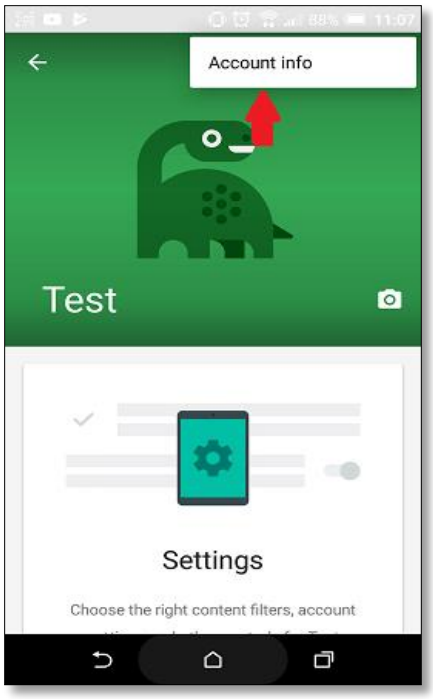


Figure 227 Select account info to alter the account information for your child.

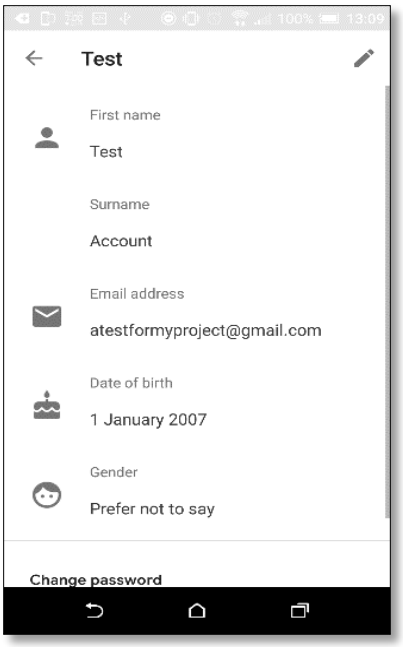


Figure 228 Here we can access and alter the account details of our child's account. Including changing the password and deleting the account should we desire.

Returning to the main child account management screen, the first option available to us is the ability to add a profile picture for our child or remove one if it is deemed inappropriate.

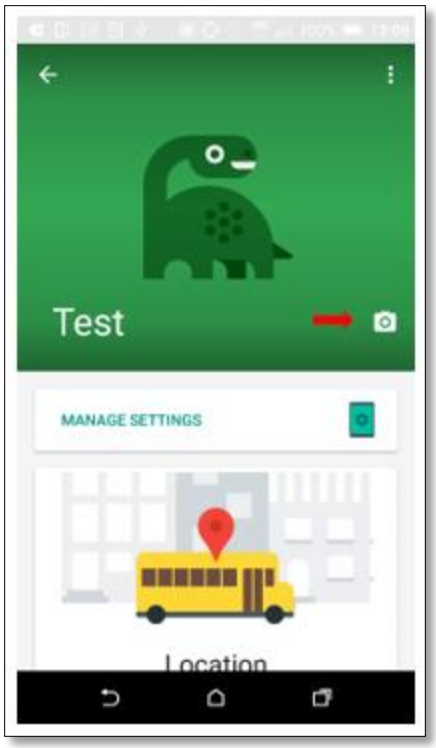


Figure 229 Here, we can manage the profile picture for our child's account.

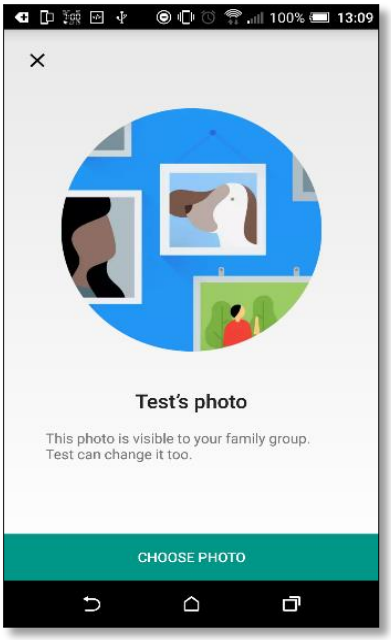


Figure 230 We can now add a profile picture, however, as this is a child's account we have elected not to use one due to the risks associated with predators.

Returning once again to the main child account management menu we enter the parental settings. These options were previously covered during the setup however as needs may, restrictions may need to be increased or decreased as times go by.

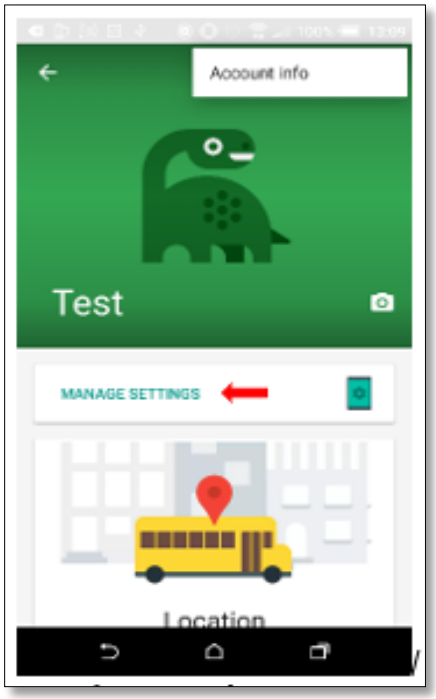


Figure 231 Here we can enter the parental settings management menu.

Within this menu we can alter the settings we selected during setup which govern age limits pertaining to Google play, movies, music and books. For demonstration purposes, I have altered the age restrictions from the youngster most restrictive age bracket to the 12 years of age bracket.

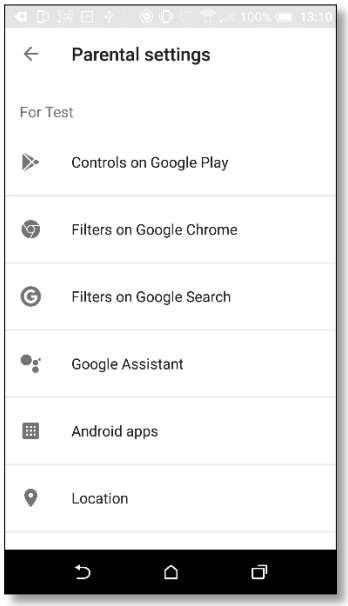


Figure 232 As you can see, we can alter the settings selected during install which govern the rules under which out child's device operates.

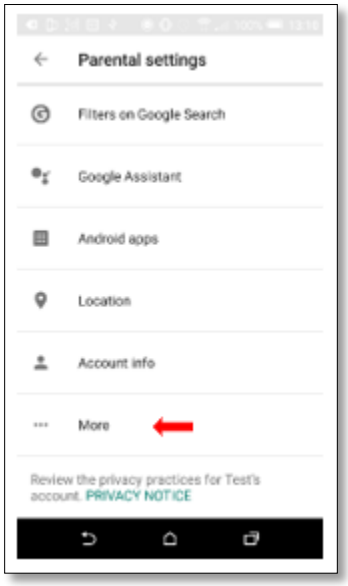


Figure 233 Further options are available within this menu by selecting "more" as seen above.

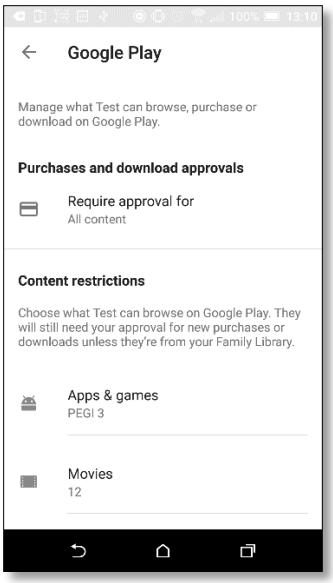


Figure 234 First, we can alter the settings relating to approval requests.

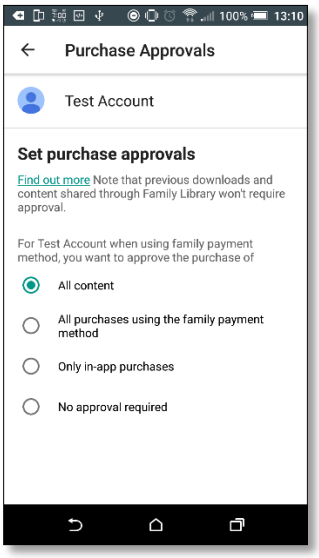


Figure 235 As you can see we elected to retain our strict settings here as this affords the highest degree of security and peace of mind for parents.

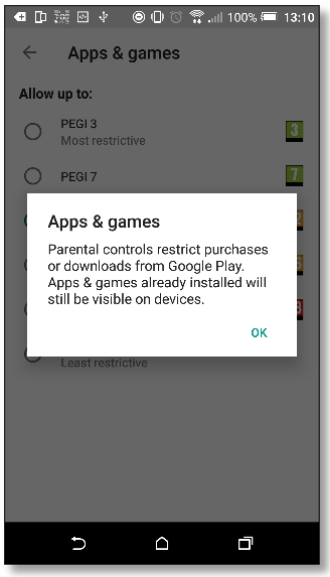


Figure 236 Here we have elected to increase the age limit on Apps, so that out child may access games more appropriate to his/her age level.

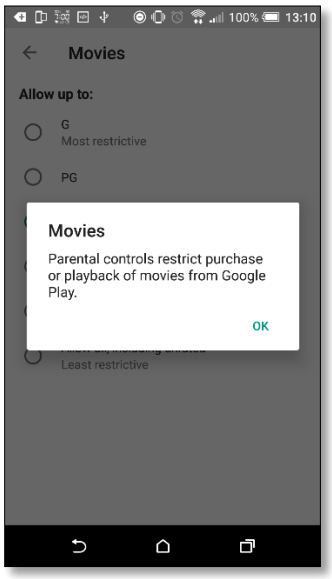


Figure 237 Again, we increase the age limit allowing access to more age appropriate movies via Google Movies.

The next setting is one that parents will have to give deep thought and consideration too. This is the third-party App setting which may restrict a child's access to Apps outside the Google Play store approval system if turned off. We recommend that this be switched off permanently and is only turned on selectively when a parent is present to physically install a non-Google store App that they approve of and add to the allowed list.

You may also add your child's account to other devices, as well retraining Google assistant to better recognize your child's voice. However, we elected to have this turned off, as we are managing the child's device and simply feel that is another data point which generates data on your child which is not necessary.

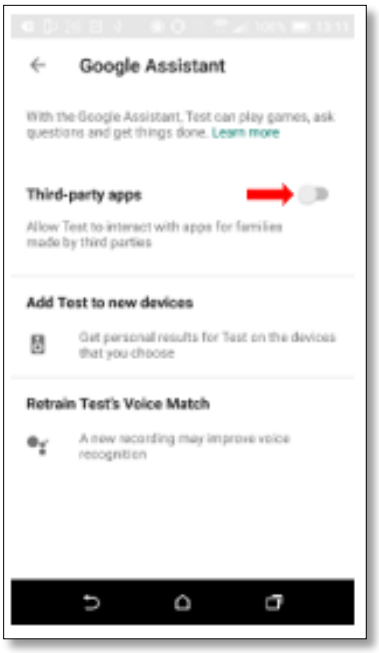


Figure 238 Here we can manage third-part Apps, add our child's account to other devices and managing the Google assistant's ability to understand and recognize out child's voice. We strongly recommend disabling access to third-party Apps.

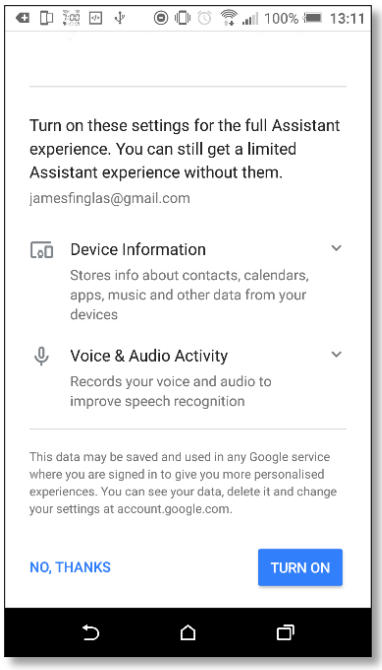


Figure 239 Here you can see the Google assistant related settings. We recommend leaving these off as they only serve to provide Google with data to collect.

Next up on the main child account management is Location settings. While we recommend leaving these off if your using any Apps, such as Snapchat which may monitor and reveal publicly your child's location, or even just their device location, parents may also wish to use this feature to track their child's location. We have elected during setup to disable this feature, so let's enable it now. Know it may take some time to connect the child's device location tracking services.

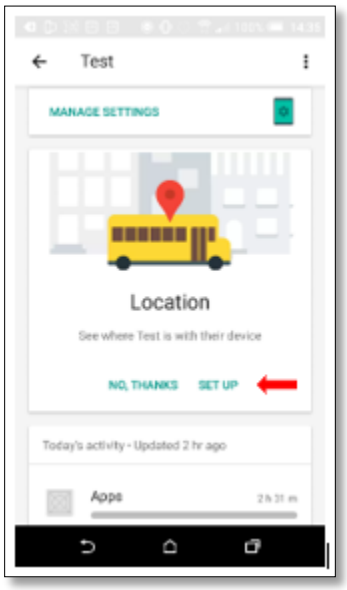


Figure 240 As you can see here, enabling location tracking is as simple as selecting setup.

Once enabled, we are presented with a map showing the device location of our child's device. We can then also add labels to important locations as we will see below.

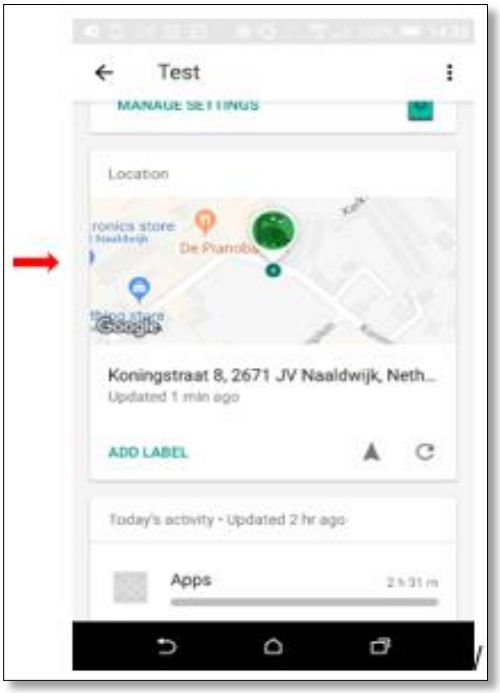


Figure 241 Here we see out child's device location! Or do we? See below for an explanation.

Keen eyed observers will note that our device is in the Netherlands. Or is it? It is not. This is because the device we are using to run our test child account is being operated on a VPN (Virtual Private Network management tool). This is an extra security precaution we recommend. However, it is outside the scope of covering Google Family-Link, so we may cover it at a later point. Where I to deactivate this tool my device location would change to Dublin, Ireland where the device is.

Returning to the main child account management menu we will investigate the next option available which is the App management menu. This provides direct access to the Apps installed on your child's device. So, let's examine an App now to see what we can do.

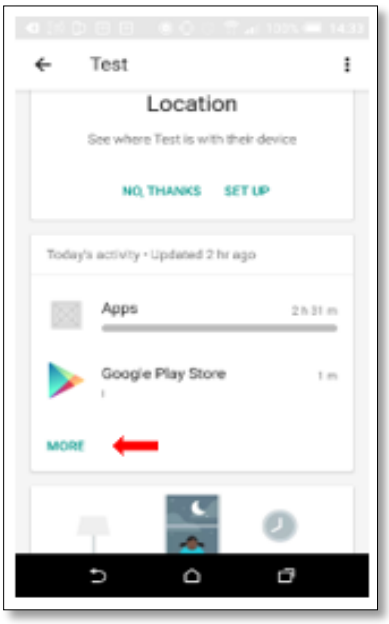


Figure 242 Select more to view the options pertaining to Apps and select the App whose settings you wish to alter.

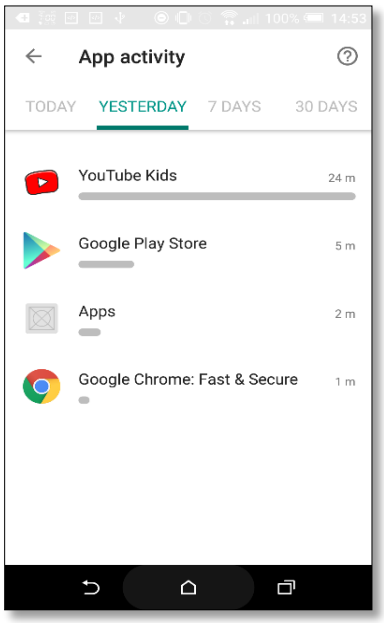


Figure 243 Here we see that we are presented with menus by time and date. We have selected 'yesterday'. And will now select YouTube Kids.

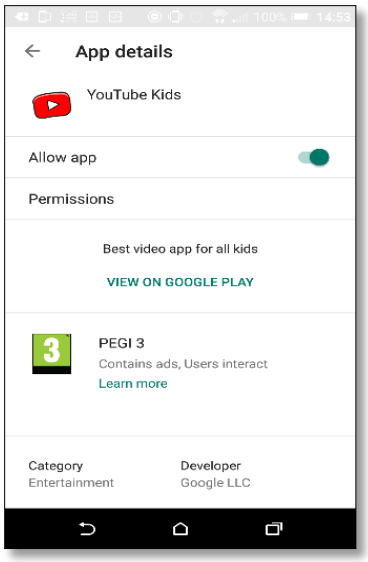


Figure 244 Here we can see YouTube Kids is selected. From here we can remove the Apps allow status and view the Apps permissions

As we see above, we can now stop the App from being allowed. This will send a message to the child's device stating the App has been uninstalled. However, the App is not actually uninstalled, instead, the child simply no longer has access to it until the parent once again allows access to it. Another very useful feature for parents.

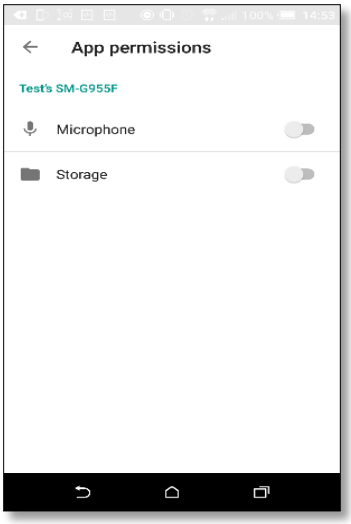


Figure 245 Here we can view the permissions the App has internally on our child's device and manage these settings.

Lastly for this section, we can manage Apps access to internal device features like the camera, microphone and storage areas of our phone. We strongly recommend that these be disabled unless necessary for an App to function.

Going back to the main child account management screen, we will investigate an option that is a parent's dream function. This is the screen management controls. That's right Parents! You can actual set time limits for your child's device after which the screen will lock. The only function of the phone that will continue to work is the ability to make calls. This is to allow the child to be able to contact the supervising adult. You have both daytime and night-time screen lock options at your disposal.

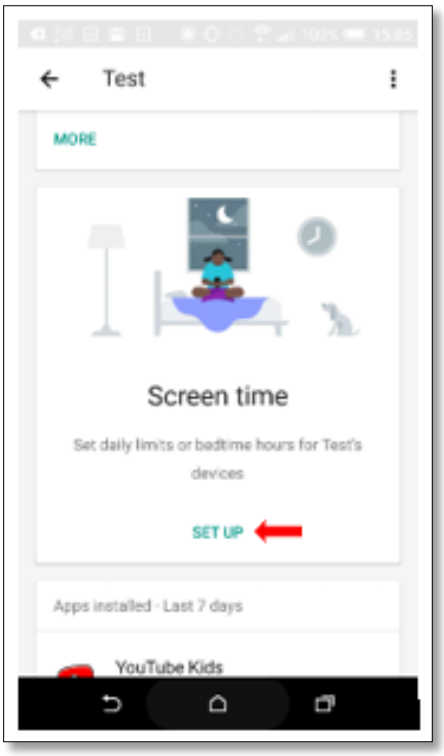


Figure 246 Here can set up the screen time locks as desired.

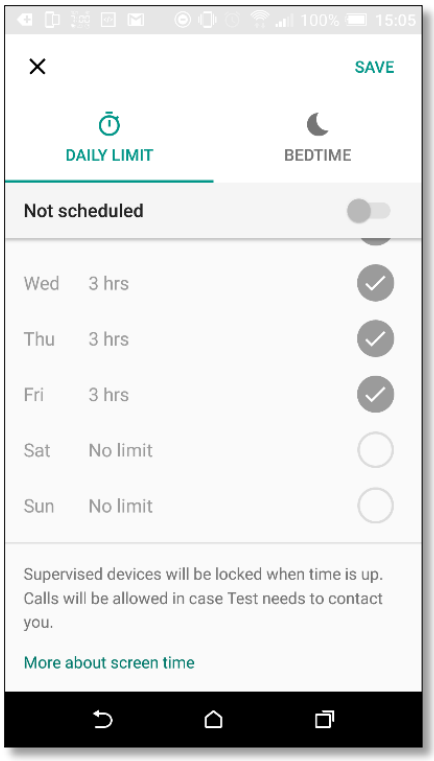


Figure 247 Here we can set up our daytime screen locks.

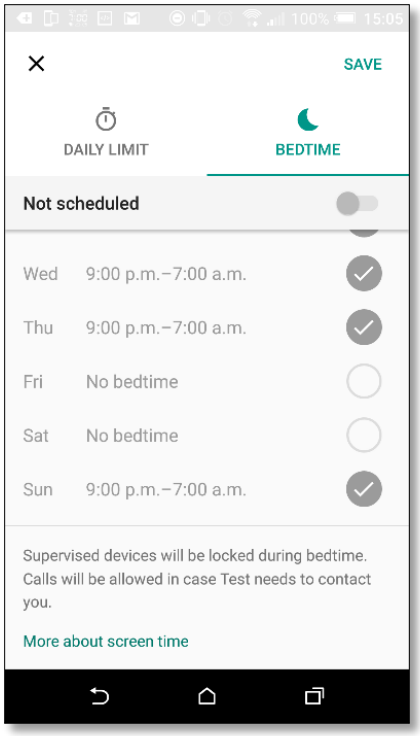


Figure 248 Here we can set up our night time screen locks.

With just a few sections left to cover It must be noted that we are going to see some repetition now. This is a comfort feature, to allow parents to access certain features from either the parental management controls, or from within the child management controls.

So, From the main child management menu we can view the installed Apps. This is another way to access and control the Apps installed on the device. This overlaps directly with the section in the parental management control menu. This is a nice quality of life feature, so the parent doesn't have to menu hop unnecessarily.

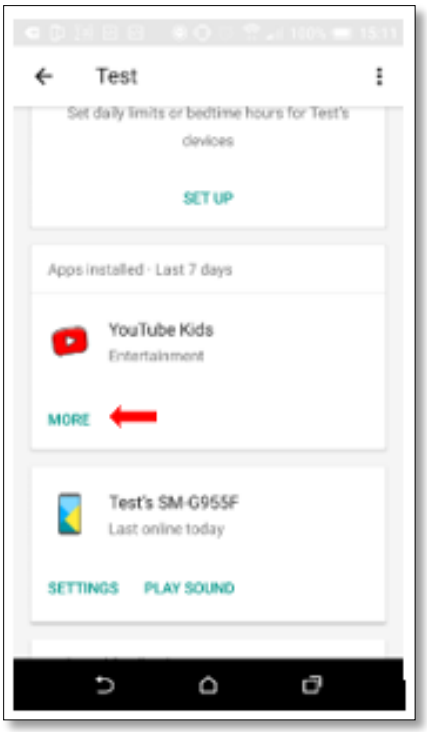


Figure 249 Here we can see secondary access provided to App settings via the child account management menu.

Now we can play a test sound which should play on the child's device to test if the accounts are properly synced and we can view some useful settings relating to the child's device, and what they can and cannot access regarding the settings on their own device.

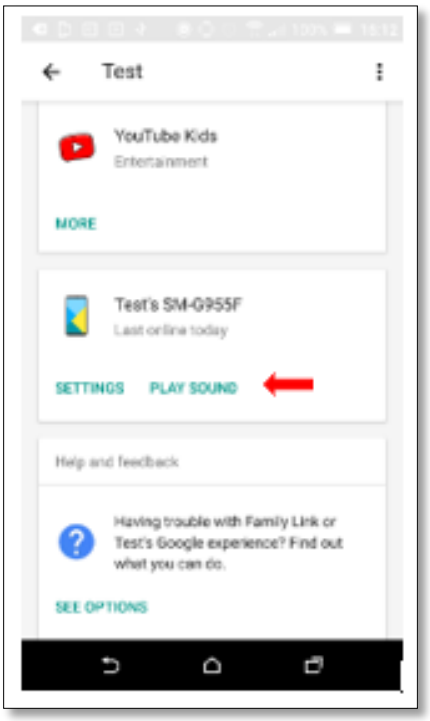


Figure 250 Here we can access some useful data relating to setting on the child's device, as well as playing a test sound to ensure the Accounts are correctly synced.

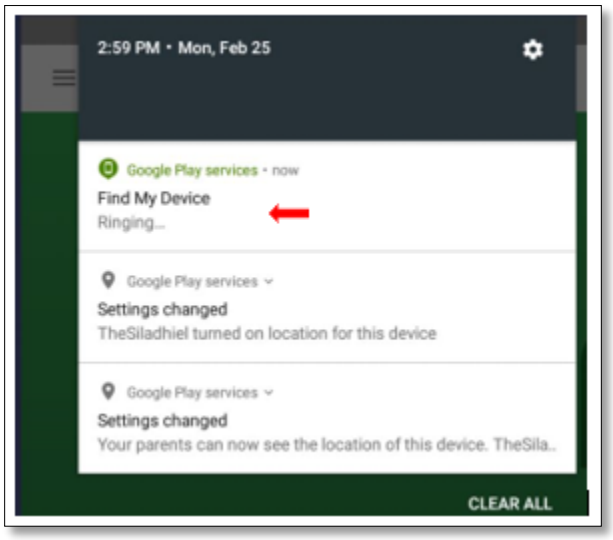


Figure 251 Here we see the test sound playing on my child's device.

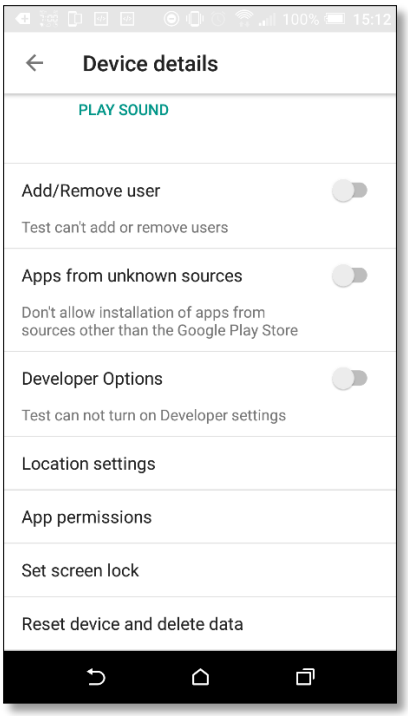


Figure 252 Here see device related settings on the child's device.

As we can see above, the child may not add or remove users, is prohibited from accessing Apps from unknown sources and can't turn on developer options. The parent may also set up a screen lock on their child's device. Lastly, in cases where the child's device has been lost stolen or otherwise compromised, should they desire, the parent can reset and erase the device remotely from this menu. Again, another fantastic security feature provided by Google.

The very last Option two option in this menu related to Google privacy terms & conditions and troubleshooting options. We strongly recommend that parents review these, knowing full well that it a thoroughly boring experience, however, your child is worth it, and it is important to know that Google take you child security very seriously. Take the time to know how the approach it.

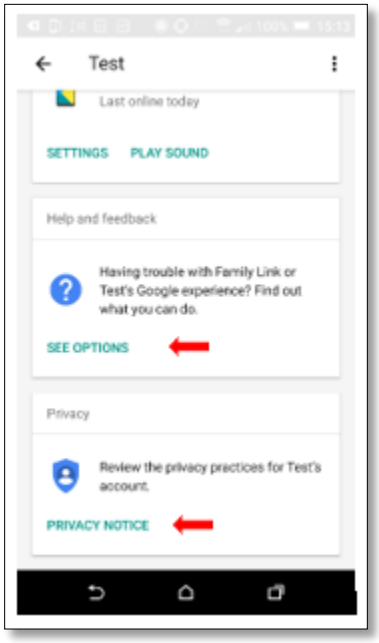


Figure 253 Here, a parent can gain access to Googles privacy terms & conditions as well as trouble shooting steps.

Child View:

The view perspective of Family-Link from the child's Perspective is, as you would imagine, highly restrictive.

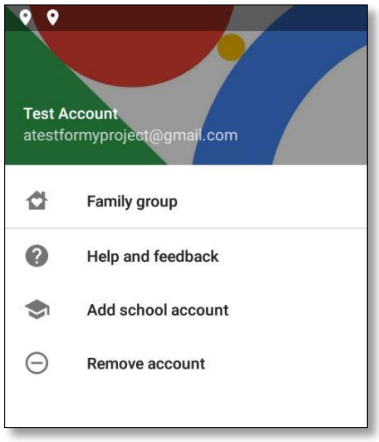


Figure 254 Here we see the menu from the perspective of the child. As you can see it is extremely limited.

All the settings seen here require the consent and passworded approval of the parent or supervisor assigned to monitor the child.

11.4.2.5 Google Family-Link Best Practice Settings Guide

Having reviewed the settings, we will now offer a best practice guide to the settings we suggest be employed to better protect the child's use of their Apps and their device to increase their safety while accessing online content via Apps:

- Family-Group: we recommend where possible having a second family member or supervisor added to your family group. This will allow for constant supervision and monitoring were needed when the primary supervisor cannot be available.

- Notification settings: While it can be off putting to have constant notifications popping up, we do recommend full notifications being turned on. This will allow all types of activity available within the platform to be monitored.

- Child Account Settings: We recommend that the Childs name be set to a pseudonym, that only those who must know the Childs alias, such a s friends or family, know. The child's real name should be avoided. Similarly, we recommend that a pseudonym email address be used. This will preclude the possibility of any unwanted e-mail contact from inappropriate users. We also recommend that the child's gender be set to 'prefer not to say' for maximum preclusion of identification. As discussed previously we suggest a strong password with upper- and lower-case letters, numbers and special characters of 13 digits in length.

- Profile Photo: We recommend that the child's real picture never be used as profile photo.

- Purchase controls: We recommend setting purchase controls to all content. This will remove the possibility of your child accidentally charging in App content to your credit card.

- Google play Age restrictions: We recommended setting an age restriction appropriate to your child's age. Do not set it higher as this may allow for the viewing or accessing of inappropriate content.

- Google Movies: We recommended setting an age restriction appropriate to your child's age. Do not set it higher as this may allow for the viewing or accessing of inappropriate content.

- Google Music: We recommended setting an age restriction appropriate to your child's age. Do not set it higher as this may allow for the viewing or accessing of inappropriate content.

- Google Books: We recommended setting an age restriction appropriate to your child's age. Do not set it higher as this may allow for the viewing or accessing of inappropriate content.

- Third Part Apps: We recommend blocking all third-party Apps and only allowing when a specific App needs to be installed and a parent or supervisor is present to install the App locally.

- Location services: We recommend turning off GPRS based location services both in the App and the Device settings. This will preclude the possibility of a child's device being leaked out through an App inappropriately. These can be turned on under certain conditions. If for example the child is trained in the use of these settings, or if a VPN is being used, or there is concern that a parent may wish to be able to track a child's device. Strong consideration must govern the use of this setting and for most cases the risks outweigh the benefits and we therefore recommend it be left off.

- Access to Camera and Mic: We always recommend access to these be blocked. Particularly the Camera which is very vulnerable to being accessed remotely.

- Screen Time settings: These are highly subjective, and we cannot give specific recommendations, except to say that we do feel that a child's time should be effectively managed and too much fun and lack of structured learning could of course be a bad thing. We recommend that each parent use these settings widely to balance a child's structured learning and fun times.

- Apps from unknown sources: We recommend this be left off at all times and only ever used if an experienced user needs to access it for diagnostic purposes.

- Developer options: We always recommend this be left off.

11.4.2.6 Google Family-Link App Safety Rating

Given the nature of the Family-Link App, being that it is a parental control App and therefore, is providing security as a service for all Apps on a given device, our App safety rating system does not apply to this App. However, as we discussed above, Family-Link is an innately secure App. No App is 100% flawless, and there are advanced ways to bypass the restrictions of Google Family-Link, but we feel that these methods will be far beyond the experience or expertise of most children and as such, do not present a large risk.

11.4.2.6 Reflections on Family-Link:

Family-link is a truly remarkable App and Google deserve to be applauded for their efforts here. The level of thought and planning that went into this App is clear to be seen and they have produced a truly fantastic security App. While the setup up does take some time, as does proper configuration, the usability is high. And the ease at which someone, even if they are not tech savvy, can understand the features is fantastic.

It is important to remember however; no App is perfect where security is concerned. And any App is only as good as the level of oversight a parent puts in where monitoring their child online activity is concerned. While Family-Link is a great App and affords a truly great level of security and peace of mind… it is only a tool to accompany great parenting practices and it should not be assumed that your child is safe simply because you set up Family-Link. You must continue to instil safe App use practices into your child and continue to teach them to try to avoid the scary dangerous parts of the internet.

We strongly recommend Family-Link to all parents, most especially those with children under 13 years of age. And while we covered it initially as it was a requirement for a child under the age of 13 to create a Google Account, we recommend it for all children even if they are not using YouTube Kids.

11.4.3 YouTube Kids

YouTube Kids is an App based off the popular YouTube App, it's focus is to provide videos safe for children. It does this by filtering out any content that may be deemed unacceptable. The App has all its content filtered into four categories, these categories are, Shows, Music, Learning and Explore.

It should be noted that explore is not a search feature but is in fact a feature where any other videos that do not fit into the other categories are placed.

The App was originally only available on Android and IOS devices, but since then it has been released for LG, Samsung, Sony Smart TVs and Android TV **(Ducard 2017)**. The App is currently region locked to specific regions if used in conjunction with Family-link, however this restriction can be easily bypassed with the use of a VPN, which allows a user to present themselves as being in another location from the one which they currently reside. VPN's also add another significant layer of added protection as previously covered. It should be noted, as previously documented in our YouTube section, traffic on YouTube is encrypted by Transport Layer Security (TLS) encryption. As YouTube Kids falls under the umbrella of YouTube, which itself falls under the umbrella of Google, this encryption extends to YouTube Kids **(Schechter E. 2016)**.

YouTube kids does not require an account to be used, however to use the settings an account must be made (This account will automatically presume the user is 13 years old or younger). The only accounts that are accepted are Google accounts, in contrast to the normal YouTube application, you are not able to upload videos through YouTube Kids. You are also not able to make or read any comments on a video. This removes the potential of encountering the toxic environment which is present on the traditional YouTube App.

If you set up a Google account for your child, it will request the use of the App Family-Link, which has already been mentioned before, and due to Googles usage policy, this is a necessary requirement.

However, if you set up YouTube Kids with your own Google account, you can set up a child account on the YouTube Kids App, this child account is linked to your Google account, however this is less secure than setting up an account through Family link for reasons that were previously mentioned.

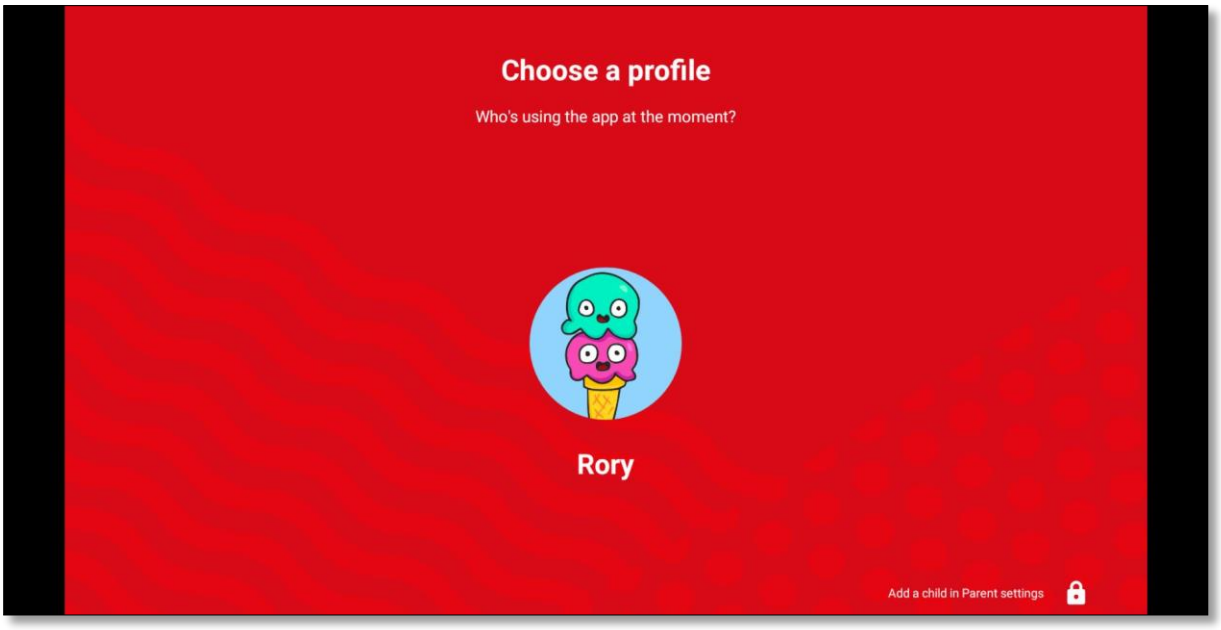


Figure 255 Here, we see the profile selection page on YouTube Kids

It should be noted that during the research of this App, a test child account was made using the name "Rory", this account is not set up through Family link.

A second account was set up through Family link, this account was set up for a child of the age of 7 years old with the name Example Username.

11.4.3.1 YouTube Kids without family link

Without Family Link:

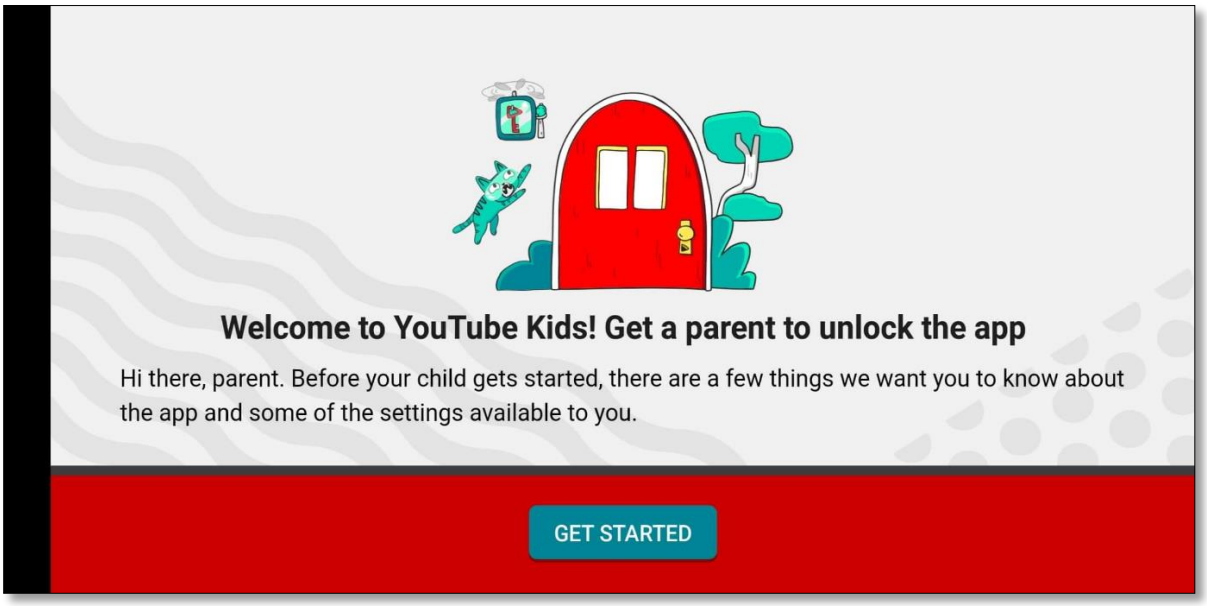


Figure 256 The Welcoming page of YouTube kids, informing a child to get a parent's permission to unlock the App.

When setting up the App in the beginning, it is requested that a parent sets up the application, it requests the parents age.

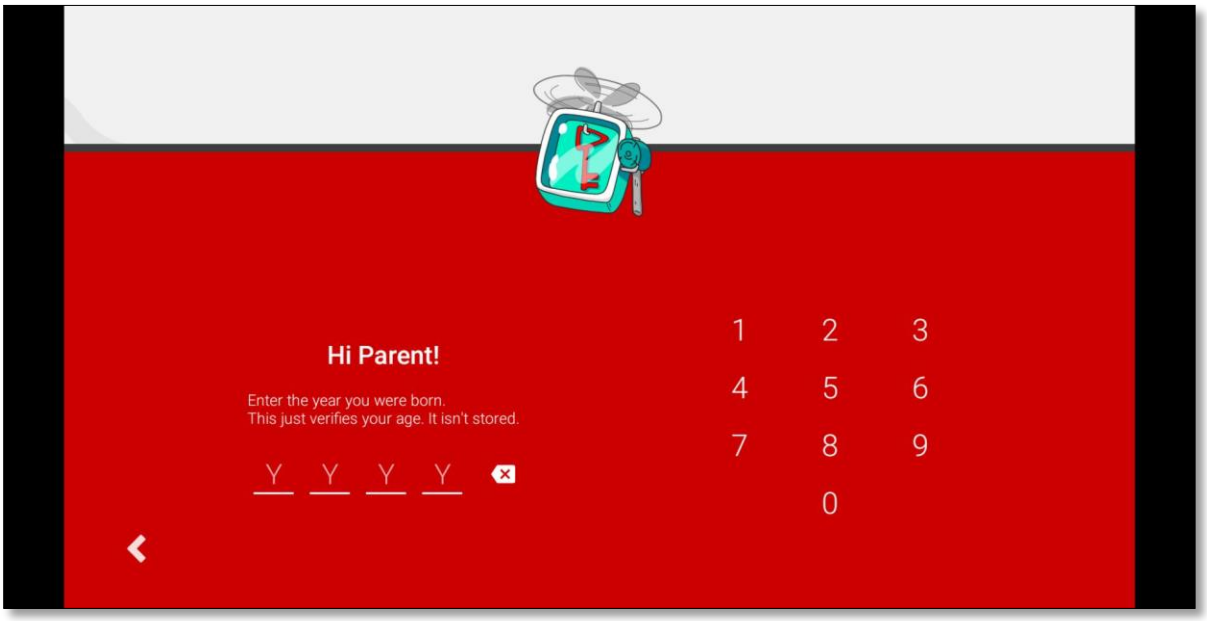


Figure 257 Here we see the application asking for the parents age

If the year provided is under the age of eighteen, then the App will ask for a simple multiplication. This multiplication question allows for multiple attempts and can be brute forced by simply guessing the answer.

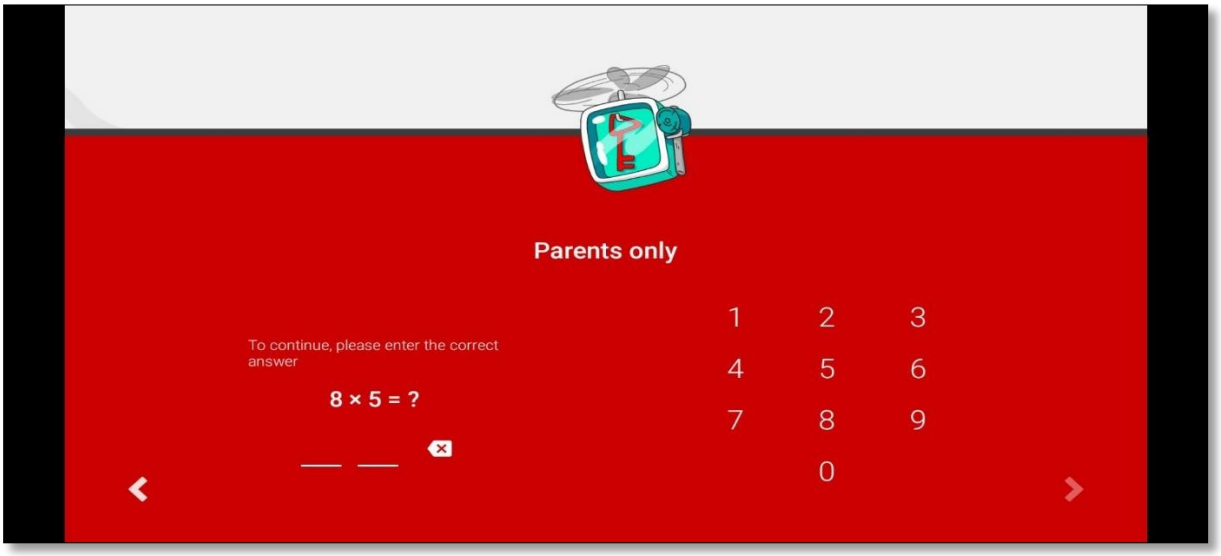


Figure 258 Here we see the application asking for a simple mathematical question

After this step is completed, the parent is given an overview of what YouTube kids is and are shown a quick guide on blocking and reporting content, teaching the parent or user how to block content which they feel is unsuitable for a child to view.

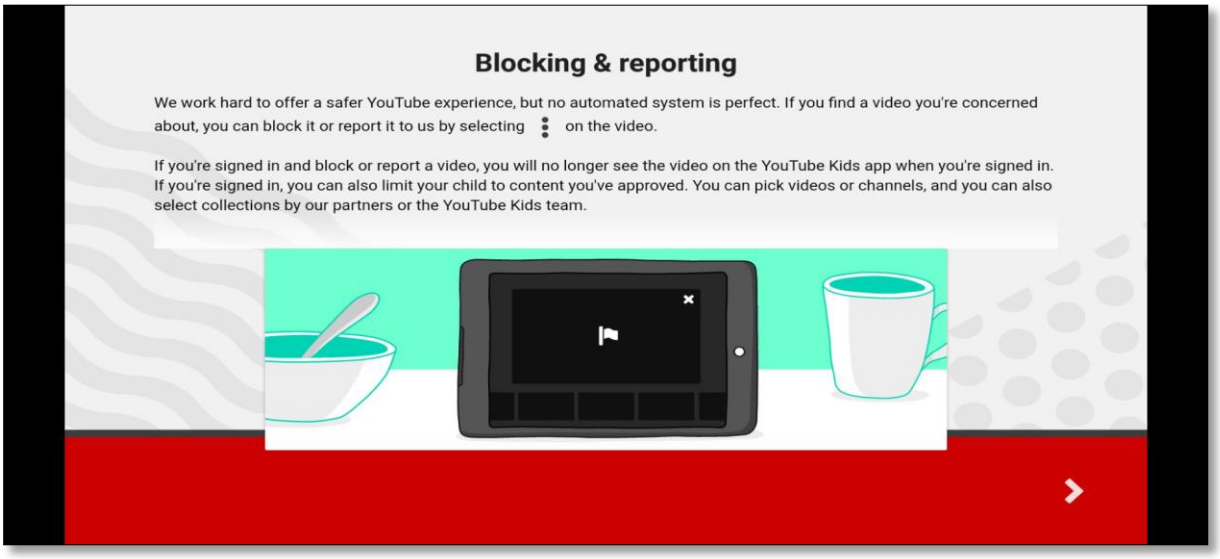


Figure 259 Here, we see the application providing information on how to block and report videos on the application.

It also requests if a child should be allowed to search for content on the App, or to only have access to suggested content. It is requested to add an adults account; however, this step can be skipped.

11.4.3.2 YouTube with Family Link

When it comes to a child having an account under the age of 13, they are not covered under the legal digital age of consent, and therefore the Google corporation cannot be held responsible for any unfortunate incidents that may happen as a result of using the App, with the addition of Family-Link you are able to take over the settings and restrict Apps to further attempt to prevent any unfortunate incidents from taking place.

YouTube Kids is one of the Apps that can be set up with connection to Family-Link, however when it comes to settings, it becomes a lot more difficult to set up. At the current time of writing this paper, connecting Family- Link to YouTube Kids is not currently supported in the Republic of Ireland or the United Kingdom. If you attempt to set up YouTube Kids with Family Link, it'll provide an error page that search settings cannot be established.

To get around this, connect yourself to the United States using a VPN, the one we are using in this scenario is ProtonVPN, this is a free App. A VPN is a program used to connect your device to a server which forwards all traffic to and from your device. This hides the users IP address and presents the VPN's address as the users. This is an extra security layer we recommend in all cases, but for now, it's only needed for this one step.

Many VPNs require setting up an account to use, this is easy to set up, however when it comes to setting up YouTube Kids with Family-Link already installed, it requires the use of the chrome browser to set up a ProtonVPN account, which is automatically blocked by the Family Link App on the child's device, a solution to this is to unblock Google Chrome, or to set up a ProtonVPN account on a computer.

Once an account is created, you can set your location by scrolling down to the United States on the country's menu, or you can select the US on the map view, this will select an IP from the US. Making it appear that you are connected from the United States, or any other country that is covered by the Family-Link YouTube Kids pairing.

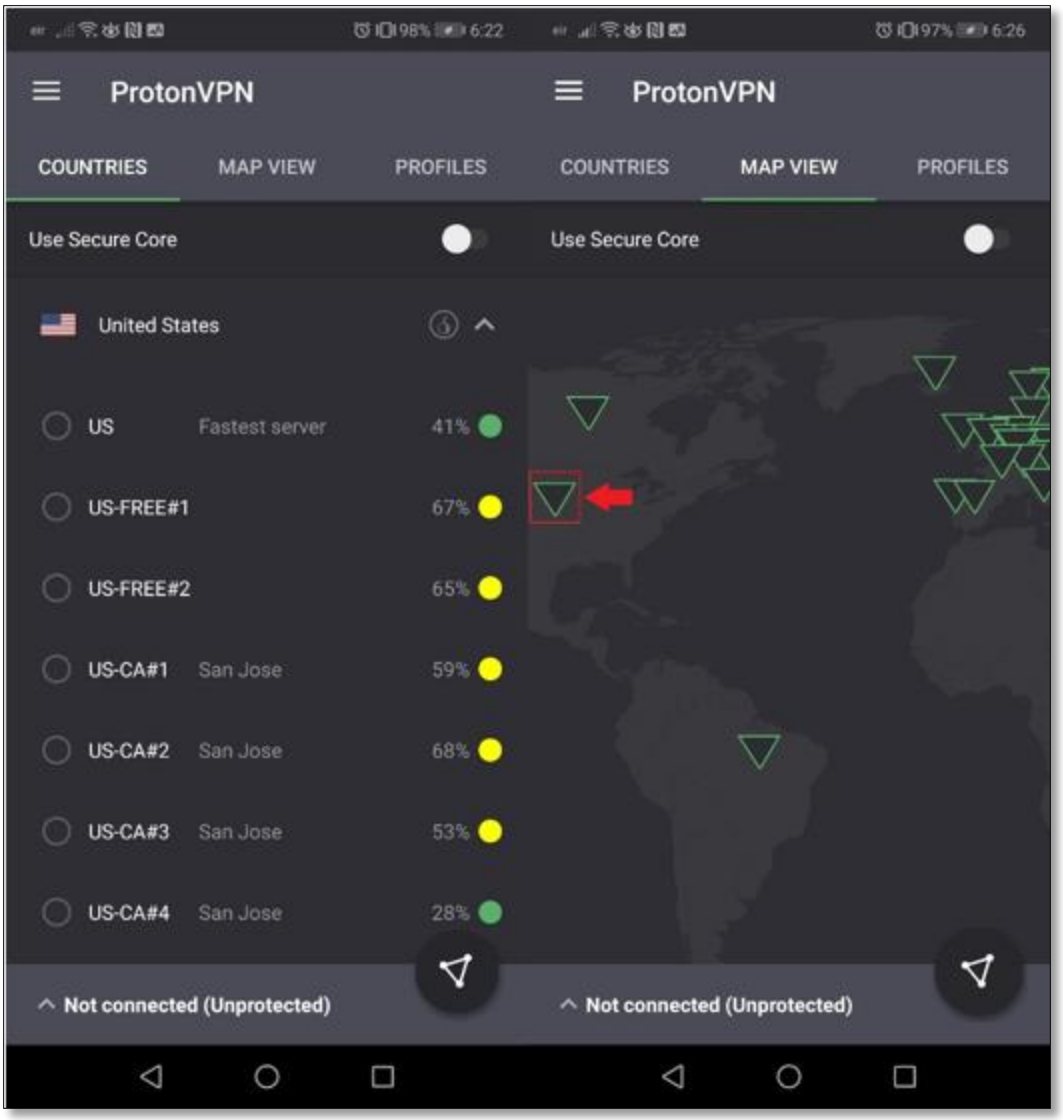


Figure 260 The implementation of a VPN

With all these set up, you should be able to set up YouTube Kids.

When opening the YouTube Kids for the first time, the first prompt is to sign in with the parents account, instructing that the App must be set up by an adult, when a parent has entered their details, they are prompted for the child's age set, the first being younger, which is for 8 years and under, while the second being Older, which is between 8 to 12 years old.

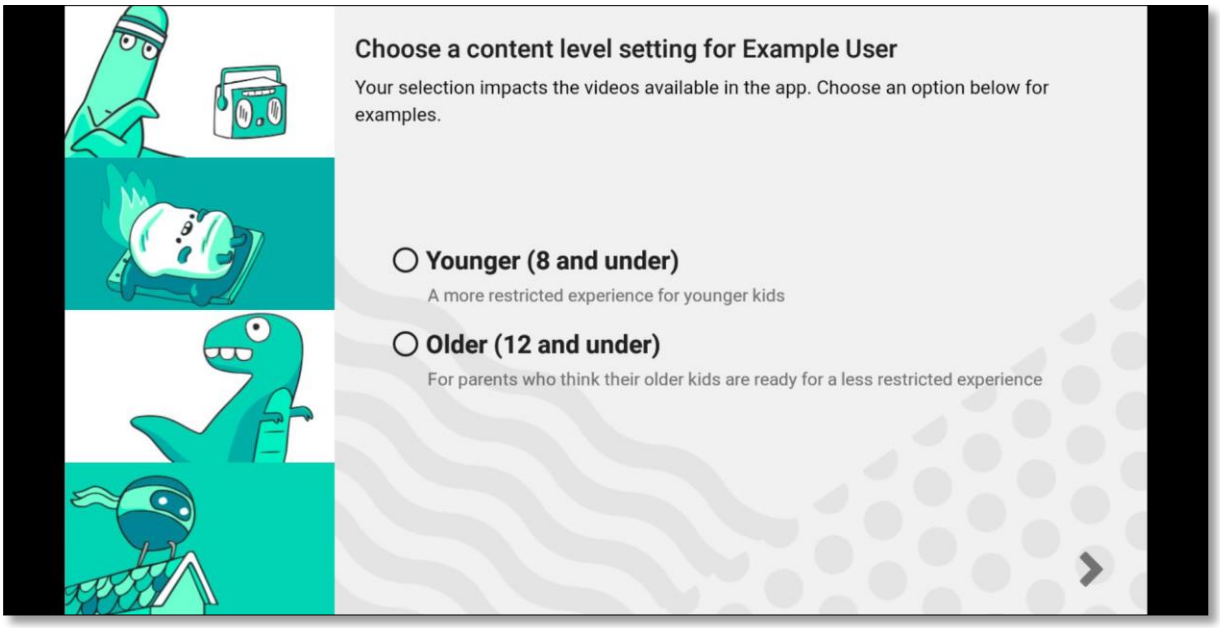


Figure 261 Choosing the age range of your child.

This setting allows to set a default set of restrictive rules, based on the age bracket of the child.

After this feature, the set-up proceeds as it does without having Family-Link, however, it does not require setting up of an account, due to being previously connected by the parent account.

After doing this initial set up, the VPN will no longer be needed.

11.4.3.3 YouTube kids features without Family Link

To access the settings on this App, there is a button on the bottom left of the main menu, when you press this options button, you are greeted with a mathematical question in order to prove that you are old enough (as previously mentioned, this can be brute forced). There is also the option to set your own 4-digit passcode.

Figure 262 YouTube Kids maths-based challenge code.

After entering in the correct answer, you are given three options; Settings, Timer and Feedback.

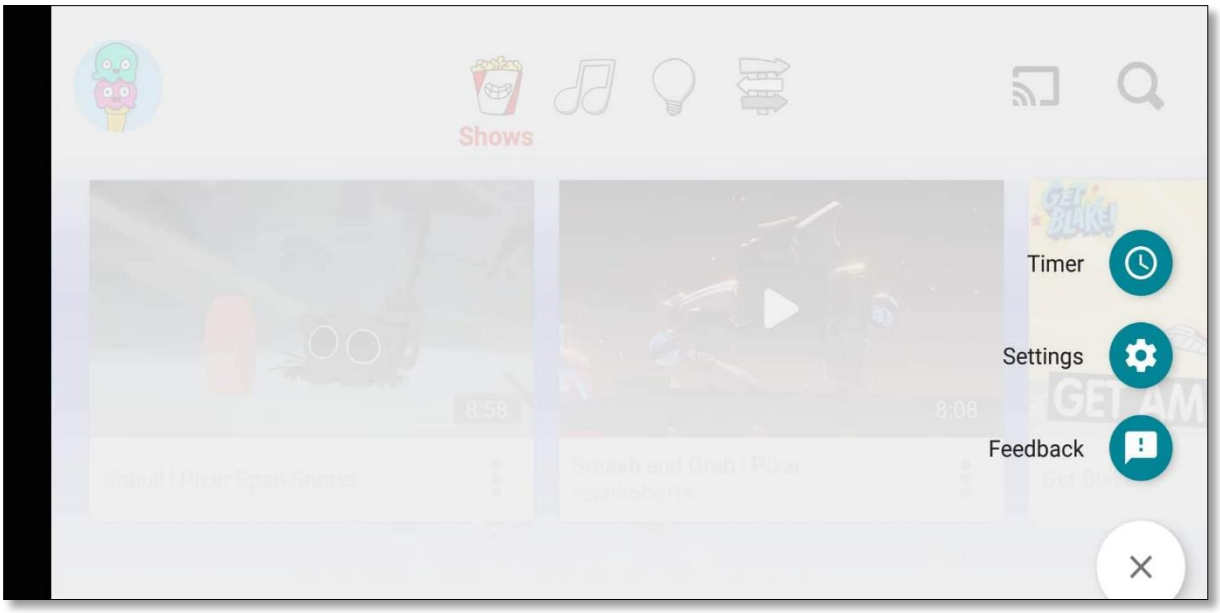


Figure 263 YouTube Kids parental options.

The timer allows for the parent to set an amount of time that their child can use the App, allowing a parent to regulate how long the child use the App. The second option is the settings menu.

Figure 264 YouTube Kids settings menu.

In the settings menu, it gives you the ability to modify your child's account, this section allows you to choose if your child can search with his or her account, allow for only content that you approve of to be viewed, to clear the watch history which will as a result reset your recommended, and to pause your child's history, as to stop recommended videos based on your child's video history. To access this section, you must provide your Google Account password.

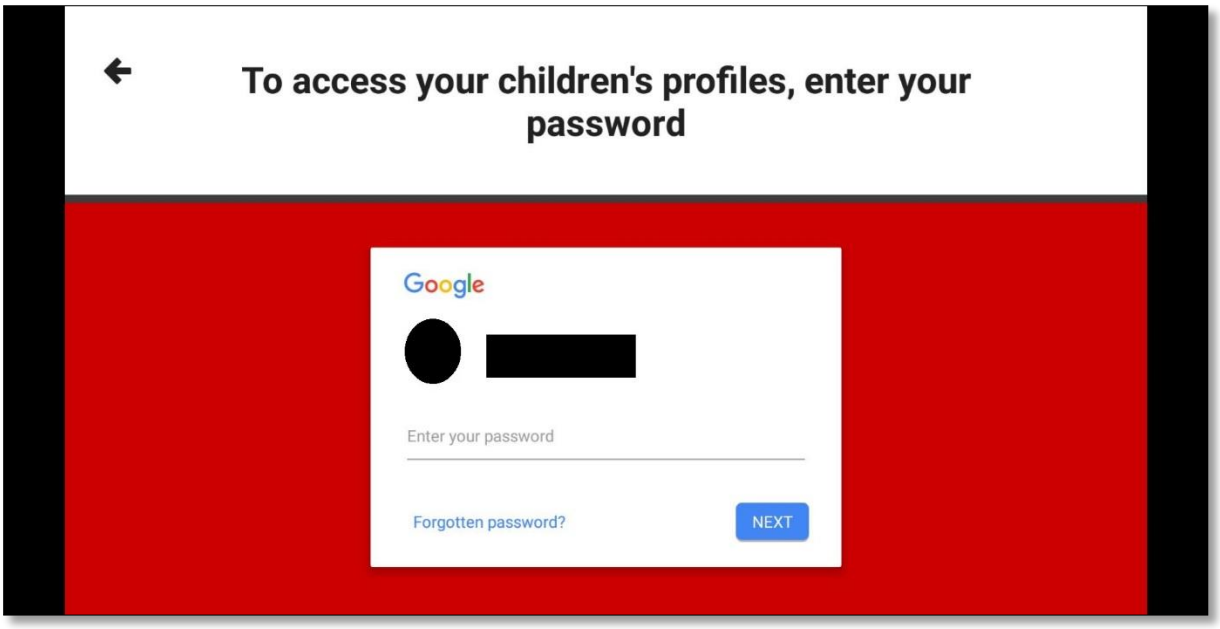


Figure 265 Entering your parental password to access restricted settings

It also allows for your child to put a secret code onto their account, so no one else can access their account. Other options in the menu is the add/change or delete the parental password and to unblock all videos.

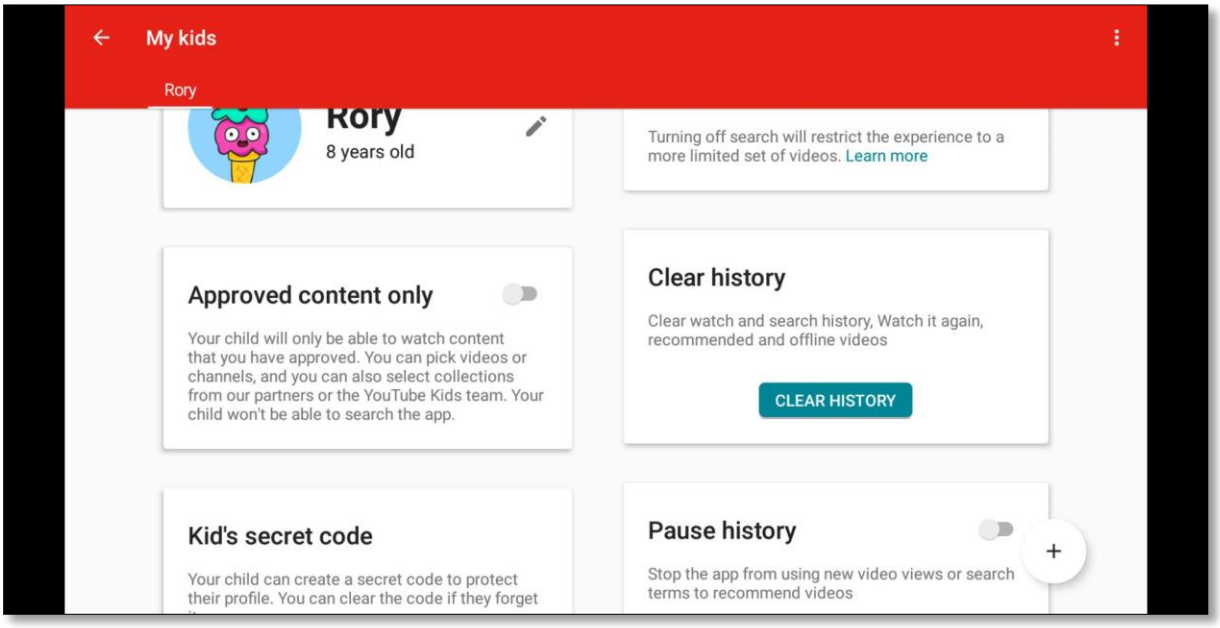


Figure 266 Further parental options.

When the Approved Content only option is activated, you are led to a section where you can choose content that you find appropriate, the content is selected by groups that is based on themes, you can choose channels from these sections.

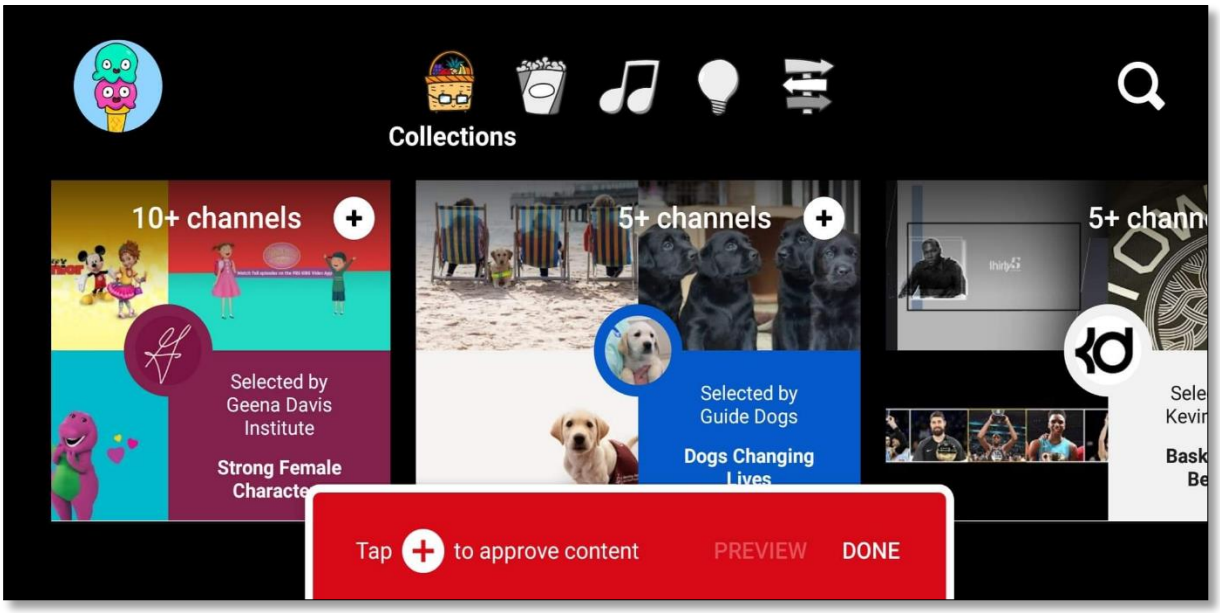


Figure 267 Content selection from channels based on themes.

This can be useful to parents who wish to block any content the parent wishes for their child not to see. There is a second menu within the kids' section on the top left by clicking the user's icon, this section does not require a password. This section has menus that were available in the other section, but they are not guarded by a password.

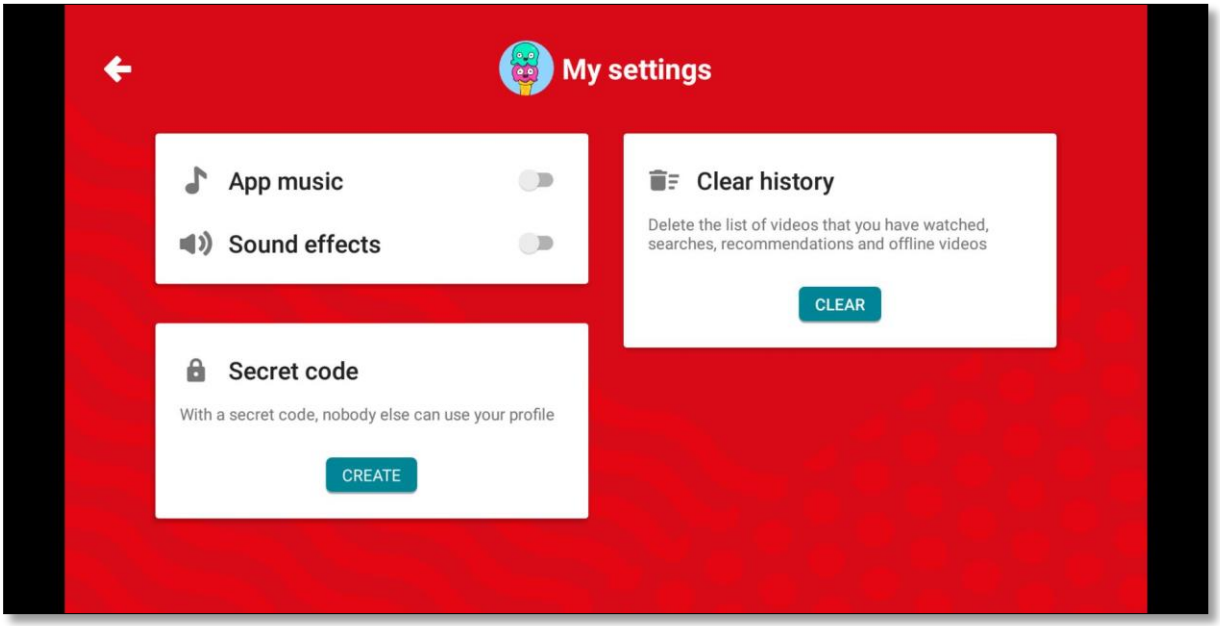


Figure 268 Quality of life access to previous settings, no longer password protected not that your password has been entered.

If there is a video that your child has come across that you find unsuitable, you are able to block they video by selecting the three dots to the top right of the video and select the block feature.

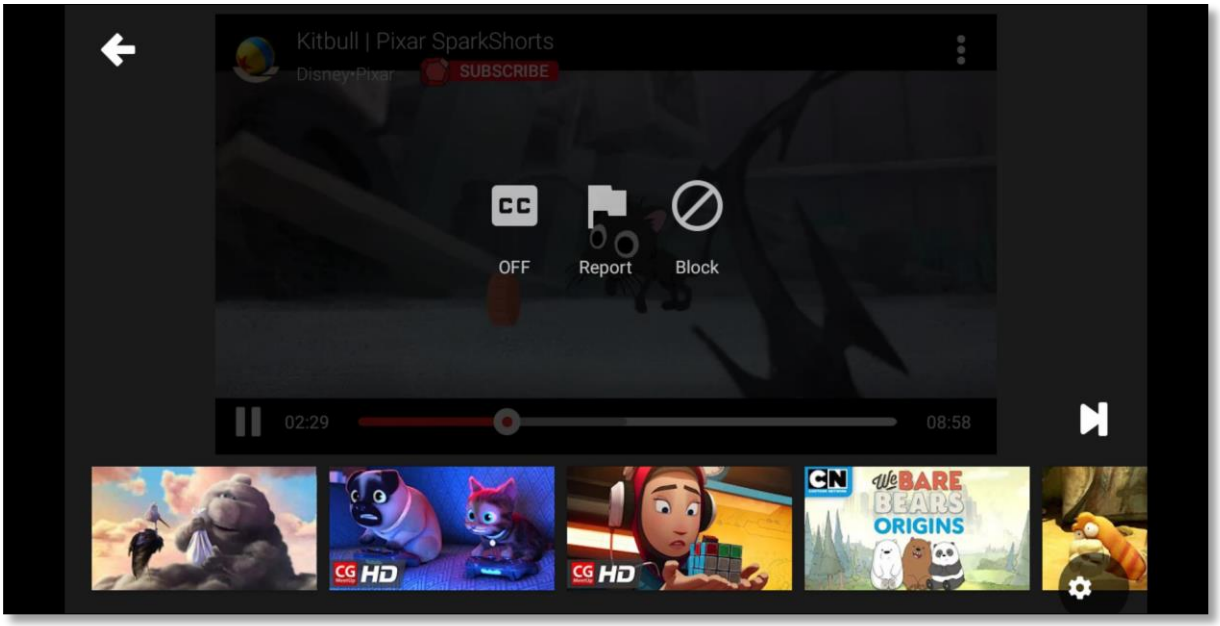


Figure 269 Manual blocking of content.

When blocking a channel, you are given the option of blocking the whole channel or just the video.

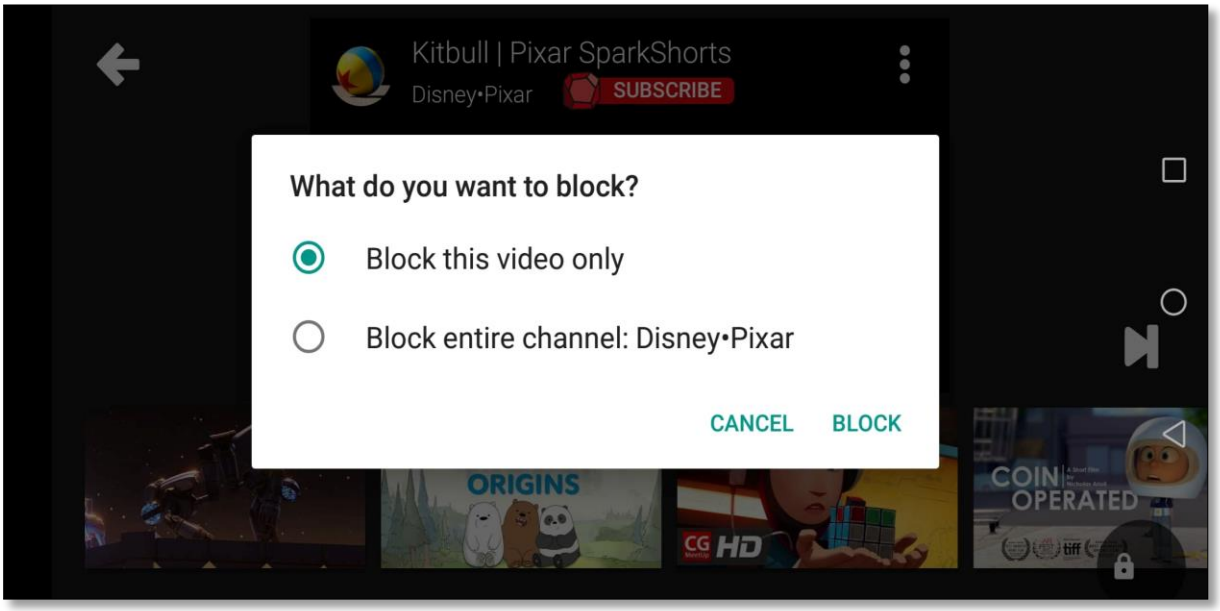


Figure 270 Blocking content by channel or creator.

When it comes to unblocking the video, you are unable to individual videos, when it comes to unblocking videos, you must unblock all channels that was blocked.

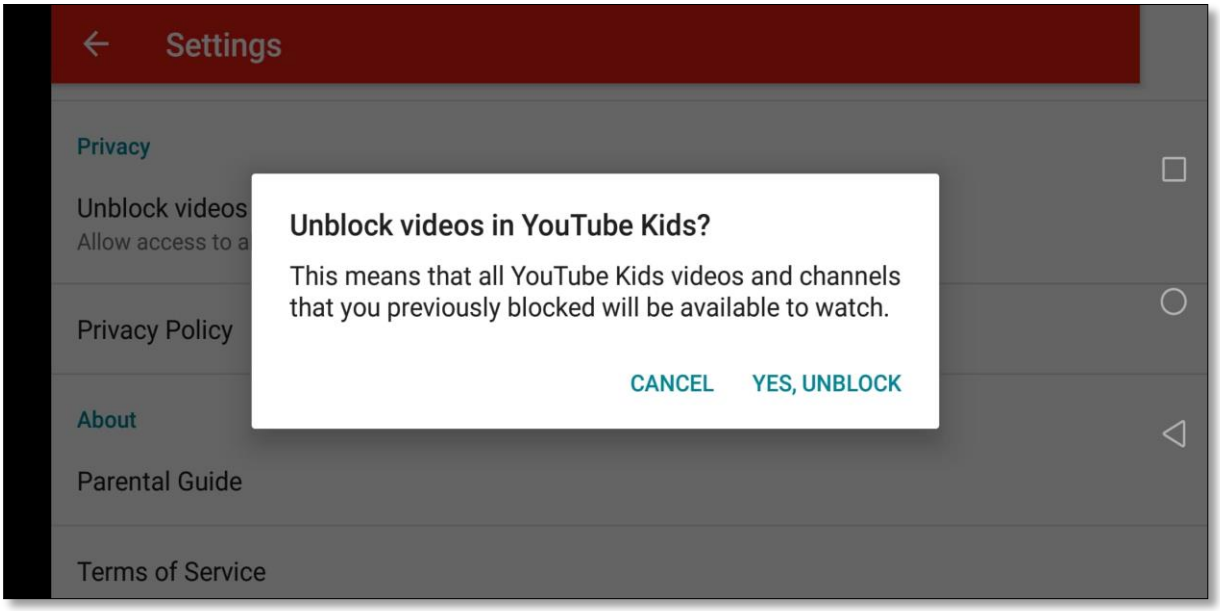


Figure 271 Unblocking videos.

11.4.3.4 YouTube Kids features with Family Link

Many of the features are left unchanged with the addition of Family Link, one major change however is that when attempting to access the settings, you are prompted to enter the parent's password instead of asking for an age or a multiplication.
After putting in the password the first time, it does not prompt for a password again, that can be considered hazardous due to the possibility of a child being able to accidentally get access to the account's settings. However, all the management of settings have been moved to the Family-Link App, and any settings that have been left behind can be reversed through the Family-Link App.

The settings that were originally accessible through the YouTube Kids App, are available by going into the Family Link App, selecting Manage settings, going to the more section at the bottom and selecting YouTube Kids on this menu.

`

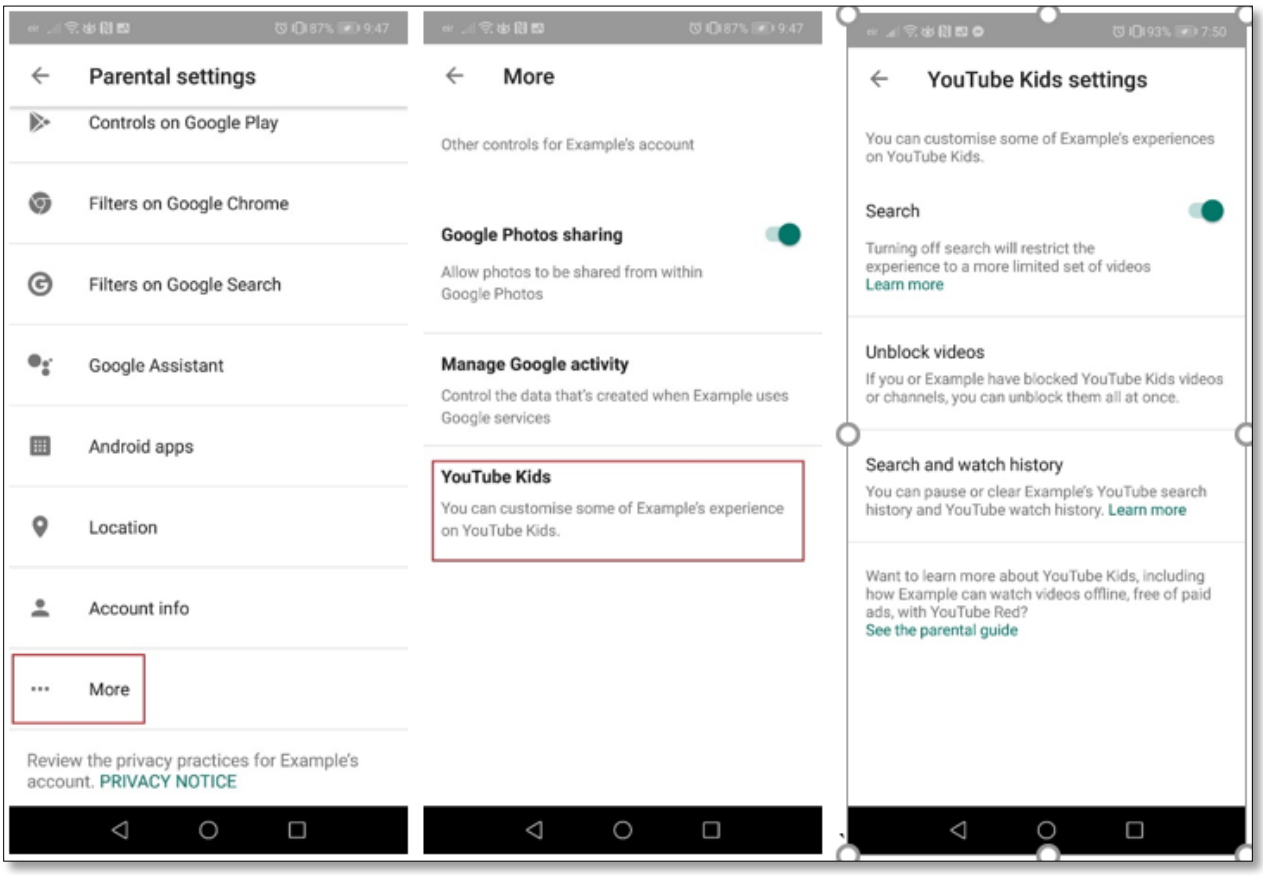


Figure 272 Managing YouTube Kids settings via Google Family-Link.

Some features remain on the YouTube Kids settings, most importantly is the ability to change the privacy settings on the App, the main problem with this is that due to the App no longer requiring a password for a parent, a child can easily stumble upon this setting.

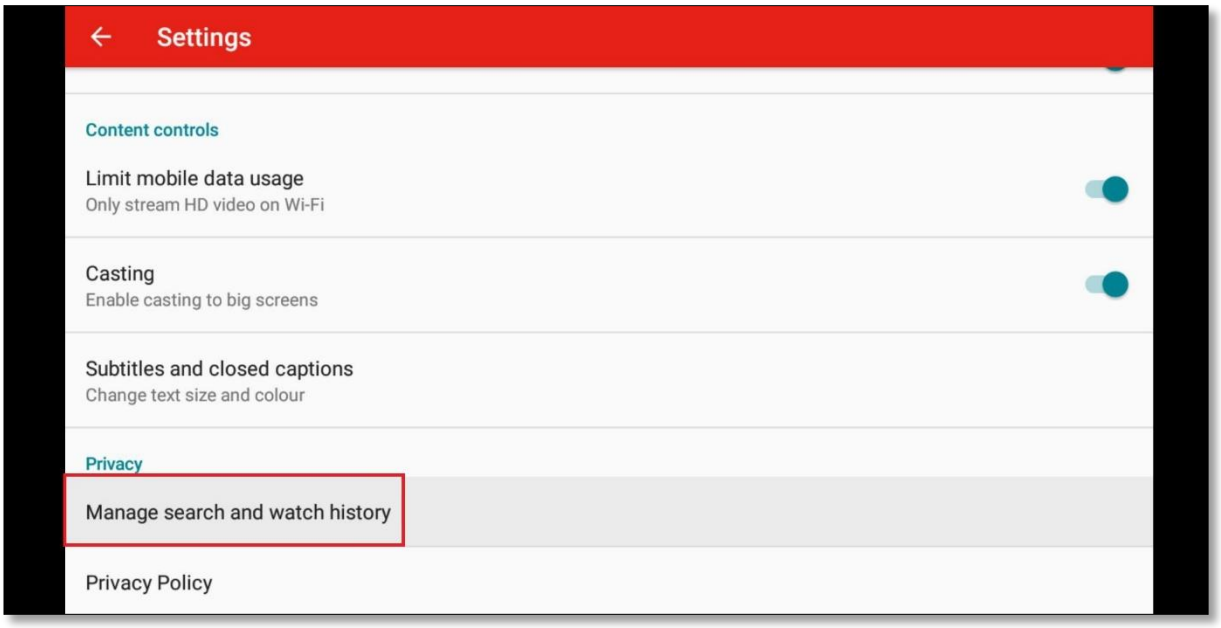


Figure 273 Privacy settings remain accessible on the YouTube Kids App presenting a potential issue.

Depending on your settings on Family-Link, you can prevent a child from having the ability to change these settings. If this feature is set that the child can edit settings, the parent will receive a notification that these settings have been changed, and are able to override these settings through Family-Link App. This greatly reduces the risk of any unauthorised changes made on the child's device.

When it comes to handpicking videos that a child can watch, this setting seems to disappear. We contacted Family-Link in order to question where this ability had gone, they had replied by telling us that it is located within the YouTube Kids section within Manage Settings, however upon inspection of this setting area, we could not find the content settings as suggested, even after re-downloading with a VPN set to the United States, we were still unable to access the feature.

However, you are still able to block videos and channels individually, this feature is still located on the YouTube kids App, however the unblock features has been moved onto Family-Link, in the YouTube Kids section.

11.4.3.5 YouTube Kids' Personal Security Optimization Options

Here are the security options for YouTube Kids

- Managing of inappropriate content (Reporting, blocking)
- Manage Search and Watch History
- Manage content (Specify what content is allowed specifically)
- Manage search functions

In the next section we will go step by step into how this is possible.

11.4.3.6 YouTube Kids Settings

When it comes to accessing these settings without Family-Link, many settings are restricted by a password from your Google account. When Family Link is enabled, most of these settings can be found on the Family-Link App.

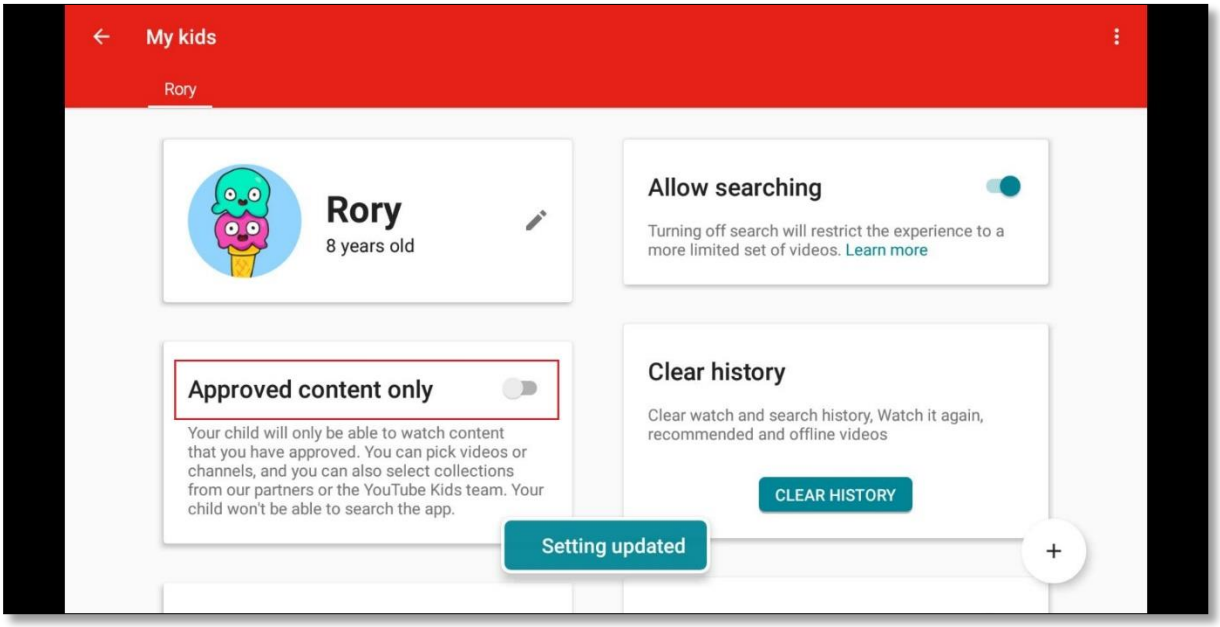


Figure 274 Accessing settings without Family-Link installed.

In this area, it is suggested to enable Approval Content Only within the 'my kids' section, picking only particular channels which you deem acceptable. This section can be found in the settings section on the App, when it is not connected to Family-Link. When it is connected to Family-Link, the setting does not appear, as previously mentioned, we have emailed Google addressing this matter, to which they replied it's a US only feature and that it could be accessed by going to the YouTube Kids section in Manage settings in Family Link. This does not appear to be the case, as even the use of VPN did not allow us to access this feature.

It is recommended to disable the search ability, as to prevent a child from searching unsuitable content, this setting can also be found in the settings section on the YouTube Kids App.

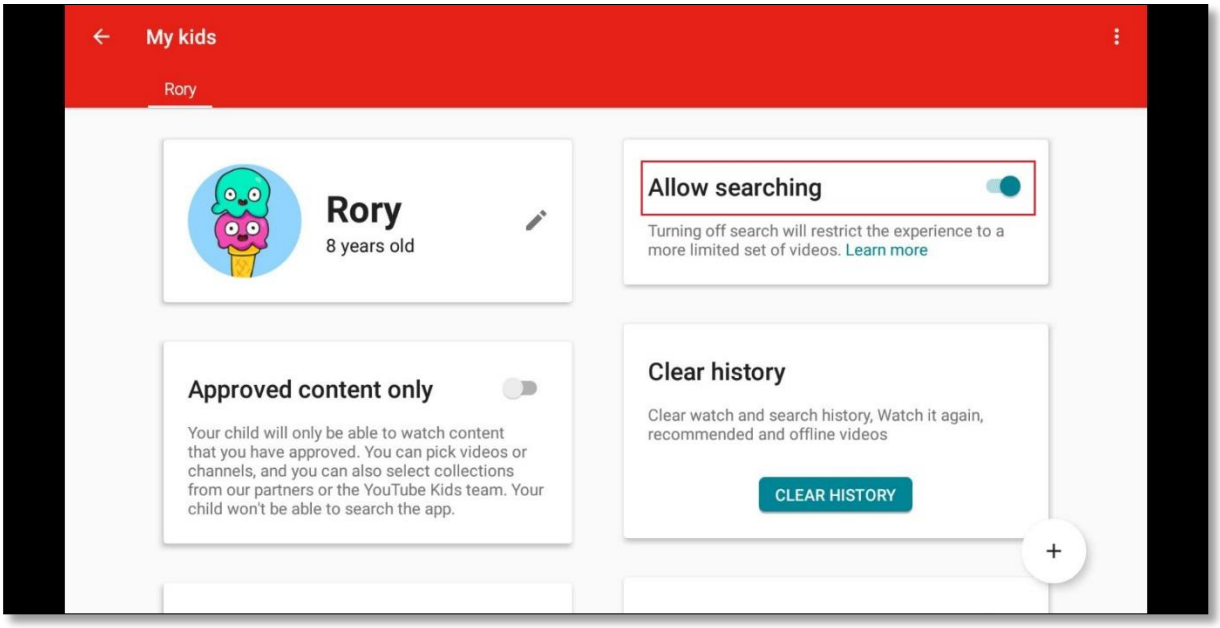


Figure 275 Restricting the search function.

When the App is being used in conjunction with Family-Link, this option can be found within the parental section of Family-Link.

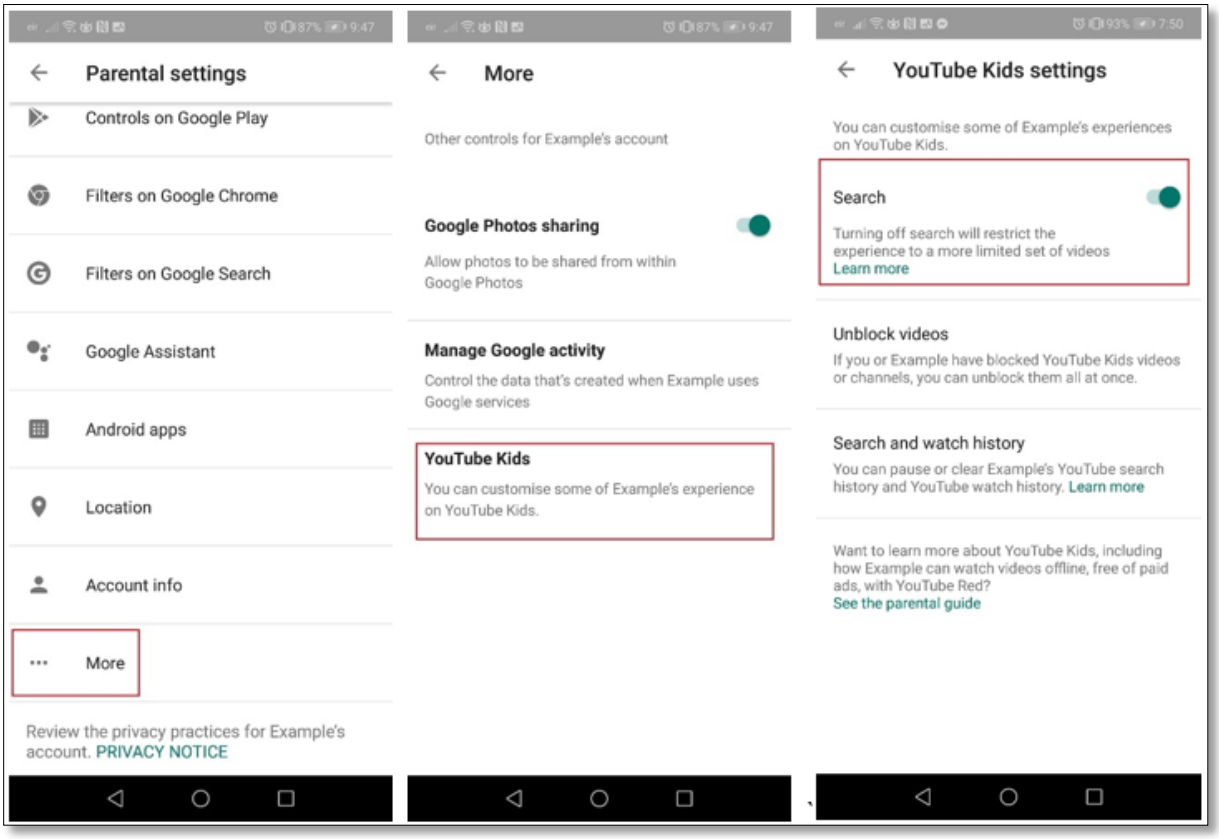


Figure 276 How to restrict the search function of YouTube Kids when it is combined with Google Family-Link.

It is also recommended for parents to allow a child to add a secret password onto their account as to give heightened security on the device, making sure that only you and your child have knowledge of this password.

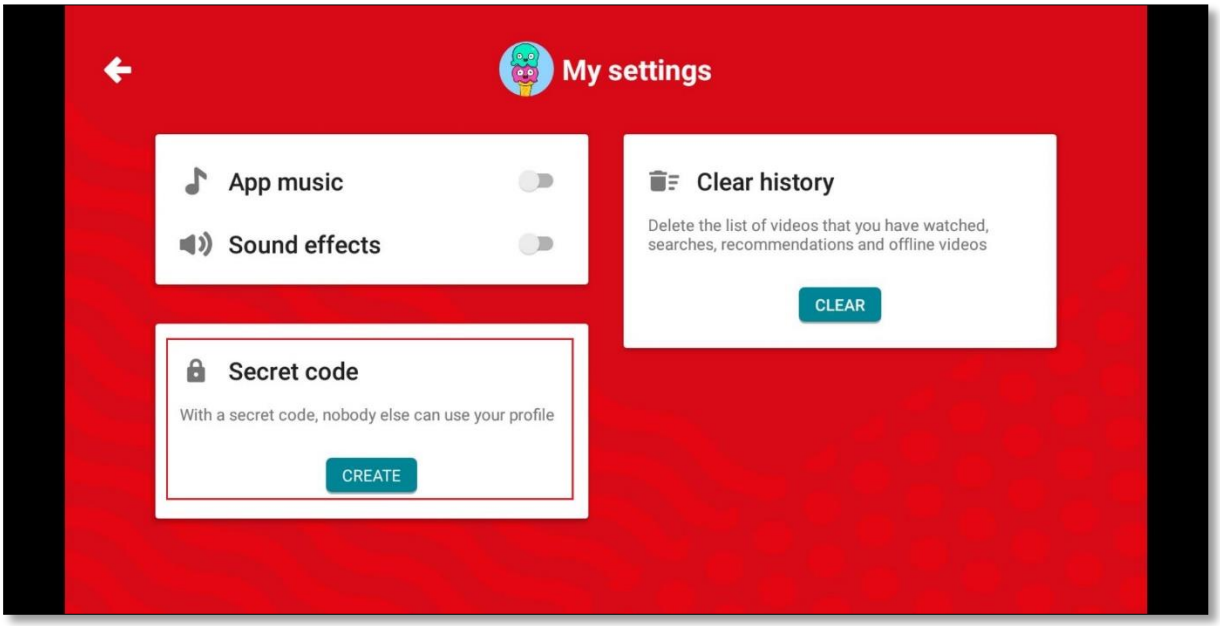


Figure 277 Creating a secret code for your child.

This ability is only available when there is no Family-Link connected to the device. However, this is understandable due to the heightened chance that this is in fact the child's own device, and thus does not need this feature, compared to if there was no Family-Link, where there is a possibility it is on the parent's device.

11.4.3.7 YouTube Kids Best Practice Settings Guide

After reviewing the settings, we've set up a best practice guide for YouTube Kids, with and without the use of Family-Link, to be able to better protect a child's use of YouTube Kids in both scenarios:

- Enable Approved Content only

  If you don't have Family Link, this feature allows you to set what content your child can view in YouTube Kids. It also disables the ability for a child to search on the app

- Enable Secret Code

  If you don't have Family Link, it is suggested for your child to be able to set up a secret code for themselves and have it so they share the secret code with only yourself.

- Disable the Search Ability

  It is suggested to disable the ability for the child to be able to search on the platform. This can be done through Family link, or on YouTube kids if you don't have Family Link.

- Block Inappropriate channels

  It is suggested to block any channels which is seen as unsuitable for children, this is the only step available to tailor content watched due to the disappearance of handpicking suitable channels.

11.4.3.8 YouTube Kids App Safety Rating

Based on our custom App safety rating system and our best practice guide being fully implemented the YouTube Kids App scores as follows.

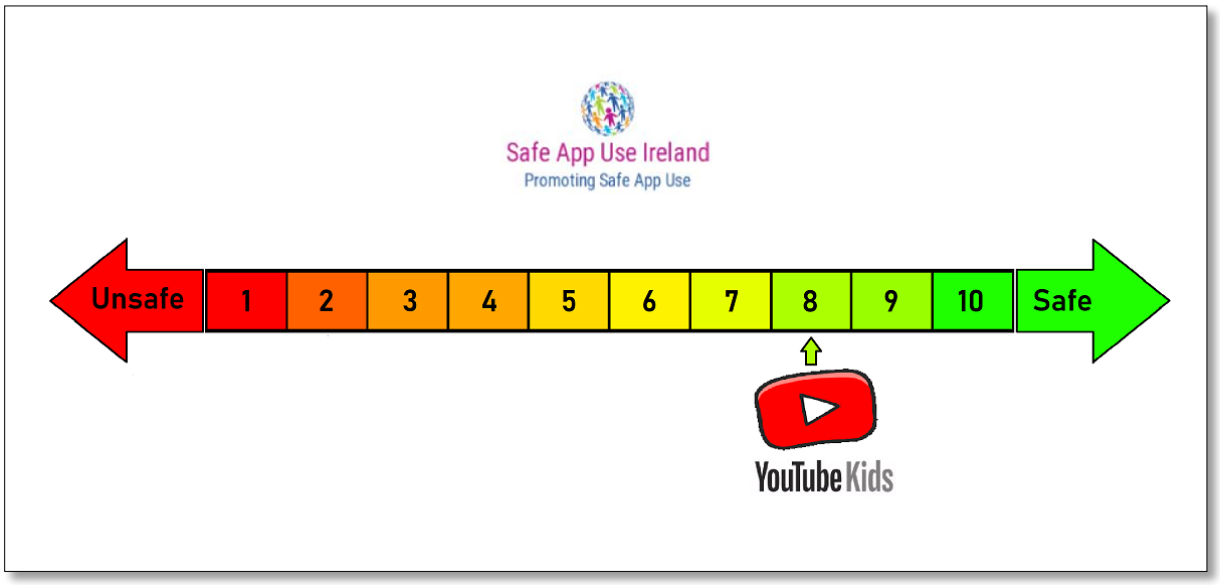


Figure 278 For Breakdown of Points System, please see: 10.0 App Safety

11.4.3.8 Reflections on YouTube Kids

Regarding YouTube Kids, we must first ask the question should we use Google Family-Link? This would depend on which device we are referring to. If we are referring to the parent's device then it would not be necessary (however in this case, maximum settings should be applied to YouTube Kids). However, if we are referring to the child's device we do strongly recommend the use of Google Family-Link.

When it comes to having the App without Family-Link, a lot of options are left open, that can be accessed by a child if they are able to get past the maths-based question, which as previously mentioned can be brute forced. This is still considered a safer option than the YouTube parent option where the options simply don't exist.

However, there are some features that disappear once the Family-Link App is installed, like the ability to handpick channels that a child can watch, instead leaving with the ability to block videos and channels (which is also available without Family-Link).

When it comes down to it, if you have a separate device for your child, setting up YouTube Kids with Family Link is recommended. But if the YouTube Kids App is also present on your device, then it is suggested to use the App restrictive settings already available on your own device, as the use of Family-Link on your own device will deactivate many features. In this case, parental supervision is recommended.

When it comes to a comparison between YouTube and YouTube Kids, we find that YouTube kids is less likely to allow for access to inappropriate content. While the algorithms are not perfect and are susceptible to manipulation, it is less likely to offer ease of access to inappropriate content. This provides a greater level of peace of mind for parents. The lack for commenting on the platform makes the platform far less toxic than its parent application, YouTube.

The ability for a child, not restricted by family, to create a YouTube Kids account that is restricted to YouTube kids and does not fall under the Google umbrella vastly decreases the online visibility of the child, the footprint left by the child any potential access a predator may have through the use of a google account. While our group does feel that YouTube kids combined with family-link is the more secure option, YouTube Kids is felt to be a relatively safe App.

12.0 Website

We elected to use a website as, in this hectic modern digital age, it is the fastest and easiest way to disseminate information o as wide a group as possible, while providing ease of access whether it be via computer, or mobile device.

The use of a blob was also viewed to be the best option, over a full blown website as it provided the easiest means of ensuring GDPR compliancy, whilst also providing accessibility to the content and the content producers. To ensure the relevance of any future content added beyond the project phase of this project, should we decide to maintain, or even pass the platform off to another group to maintain, we needed to ensure the exchange of information was a two-way street. Parents and indeed children would need to be able to comment on and critique our current work. We would also need to be able to ask which Apps Parents or Children would like us to cover next.

12.1 Goal of Website

The goal of the website is to provide our information on Apps. We will provide information on the risks associated with App use along with case studies regarding the risks. We will provide information and tutorials on how to set up the Apps in the safest manor using in App settings. The main goal of this website is to present all this information in an easy to understand way and make the navigation of the website simple without confusion.

12.2 Design Phase

For our blog we intend to use WordPress as our primary Development environment for our delivery Platform. Umlet will be used to document our design phase. Our blog is hosted by Blacknight.com. The following WordPress Plugins will also be used:

- Akismet Anti-Spam: Protects our blog from spam.
- Astra Starter Sites – Elementor, beaver Builder & Gutenberg Templates: Allows us to import free sites build with Astra theme and allows use of the builder Elementor.
- Astra Widgets: A pack of widgets for Astra.
- Better Search: a simple lightweight internal search engine for finding items within the site.
- Duplicate Page: Allows for the functionality for pages to be duplicated.
- Elementor: Comes with tools for building webpages.
- Ultimate Addons for Gutenberg: Feature rich blocks that help build website faster.
- WPForms Lite: Drag and drop form builder.

- ResponsiveVoice Text To Speech: A text to speech program designed to aid the visually impaired in understanding the text on our website.
- Yoast SEO: Search engine optimization.
- Cookie Notice for GDPR: Cookie acceptance plugin for GDPR compliancy.
- Coming Soon Page & Maintenance Mode by SeedProd
- Really Simple SSL: SSL certificate manager
- Google Analytics for WordPress by MonsterInsights: used to monitor and document analytical data scraped from the website which may be used to document future work.

12.3 Implementation

We purchased the domain name safeappuse.ie for the year. The blog will be hosted by Blacknight.com. We created a word press blog and designed our website using an Astra Starter Sites template and began adding in the content from our research paper into our website. We split the content into sections and having pictures in between. To allow for users to comment on our content we added in a comment section under our blog posts, this facilitates the blog function of our website which defines our platform as a blog rather than a website. The comments need to be approved by an admin if they are to be shown on the website or not.

Initially we found that we received a lot of spam on our website. We decided to implement an anti-spam widget called Akismet Anti-Spam which helped prevent spam on our website. We found that a lot of our pages follow the same layout, so the group installed the Duplicate Page widget which allows us to copy and paste pages saving time re-designing the layout. We designed the pages using Astra's Elementor. A useful website designer, which helped greatly as it was straight forward and allows for advanced manipulation of designing the website.

We installed Yoast SEO, which is a search engine optimizer which optimizes our website to be found on search engines based on tags and the topics we use. Because of the latest GDPR EU regulation, we were required to install a Cookie Notice on our website which tells all users that we use Cookies when they use our services. Furthermore, a data compliance disclaimer is added under all of the comment sections allowing users to see how their data is processed using the Anti-Spam filter. The Coming Soon & Maintenance mode plugin will allow us take down our site without unpublishing pages, to edit content. While in maintenance mode, admins can still view pages while logged in.

12.4 Design

Herein is documented our website design structure pre-use-test case. The Page layouts were designed to be as simple as possible with the information being easy to access via as few links as possible with no repetition of link or over lapping of content. Templates have been documented for both non-blog pages and blog pages. While subtle changes will be needed such as duplication of content or image sections, the general templates as documented below will be maintained. However, individual pages where the layout is the same but only content changes, have not been documented as this was deemed unnecessary.

The general website layout followed the following format. Our WordPress theme, Astra, comes with a default set of parameters such a green background and a 'default font size' (17 pixels). These parameters are quite awkward to alter as they begin to affect headings and links. This can be overcome with the use of custom CSS, however, that requires upgrading the professional version of our theme which we elected not to do as the cost was prohibitive. There is a further complication where by links placed inside of content sections follow the layout of the navigation bar links, so alterations to these links would have required us to redesign the navigation bar style. As the text of a link unclicked, and the background page are the same colour we had a slight dilemma. If we remained with the defaults, we cannot see our unclicked links of the page and if altered the default style, we risked ruining our navigation bar. To overcome this issue, we elected to use minor headings as in-page navigations links coupled with custom designed buttons. This decision allowed us to retain most of the default style setting of our theme while still facilitating the use in in-page links and buttons. For accessibility, usability and inclusivity we also included text to speech for the visually impaired and users who may suffer from dyslexia. This is purely a quality of life addition that we felt would be appreciated by such users.

So, our standard content font size and style remained default. The in-page links will be minor headings of size 5 or 6. We will also use custom designed buttons as in page navigations links.

The general page layout remained in line with the default style settings which came with our theme template. New sections will be added as need but shall not be customized so that the flow of the website remains as consistent as possible.

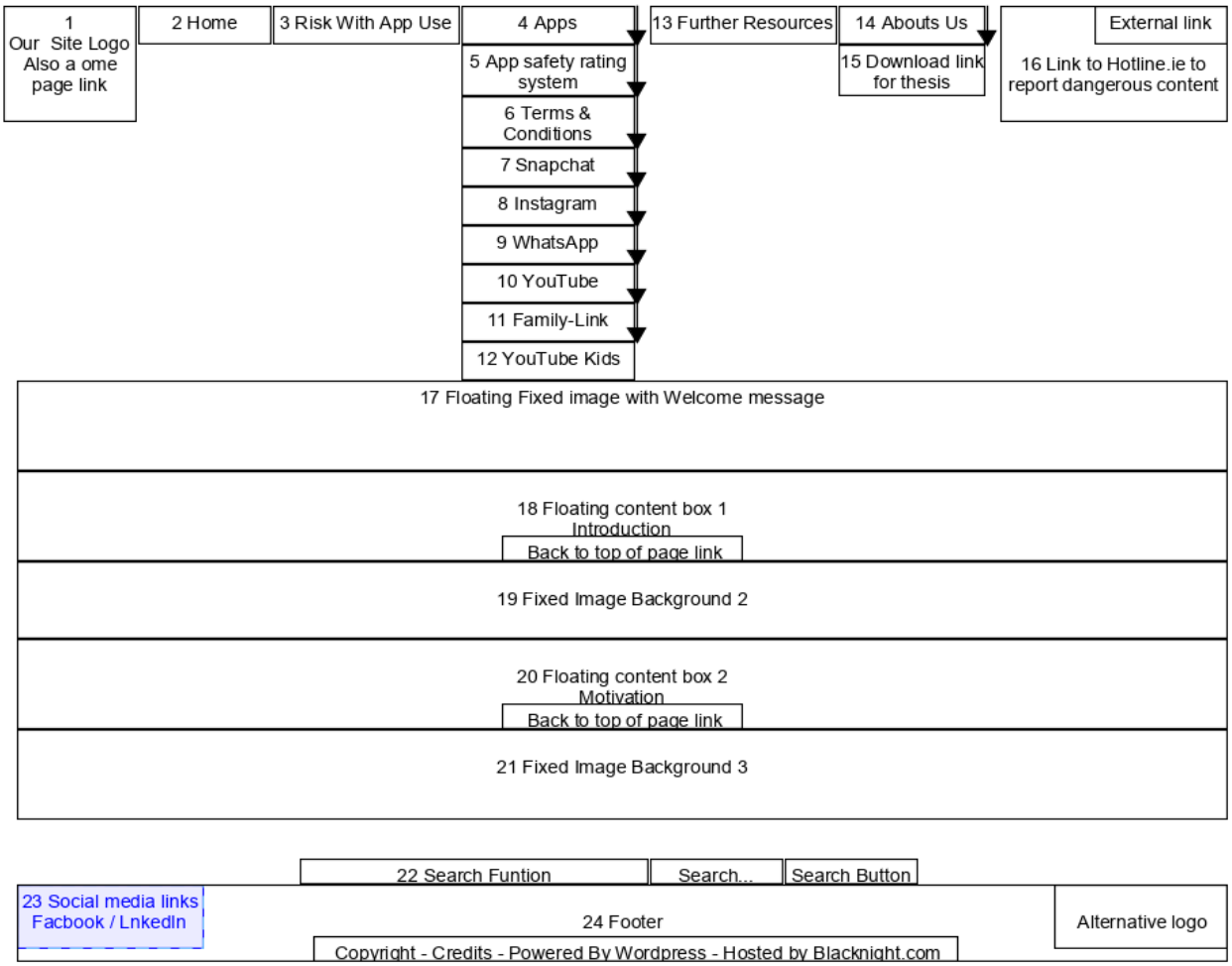
We used a custom template for all our App pages, contained within the App section of the website therefor only one of these pages was documented.

We purchased and installed an SSL certificate to ensure the security of our login information when connecting to or admin login, as well as providing peace of mind to those posting to our site. Search engine optimization was employed ensure we can reach the greatest audience possible. Google Analytics by MonsterInsights is used to document our analytical data to facilitate any future work which may benefit from this data.

Template for all non-blog pages

All pages which do not permit blog feedback will follow the following template. Content will of course vary, and the number of sections will also vary. But the template for the following pages will maintained:

- Home / Introduction
- Apps
- Credits
- Further resources
- Our research
- About us

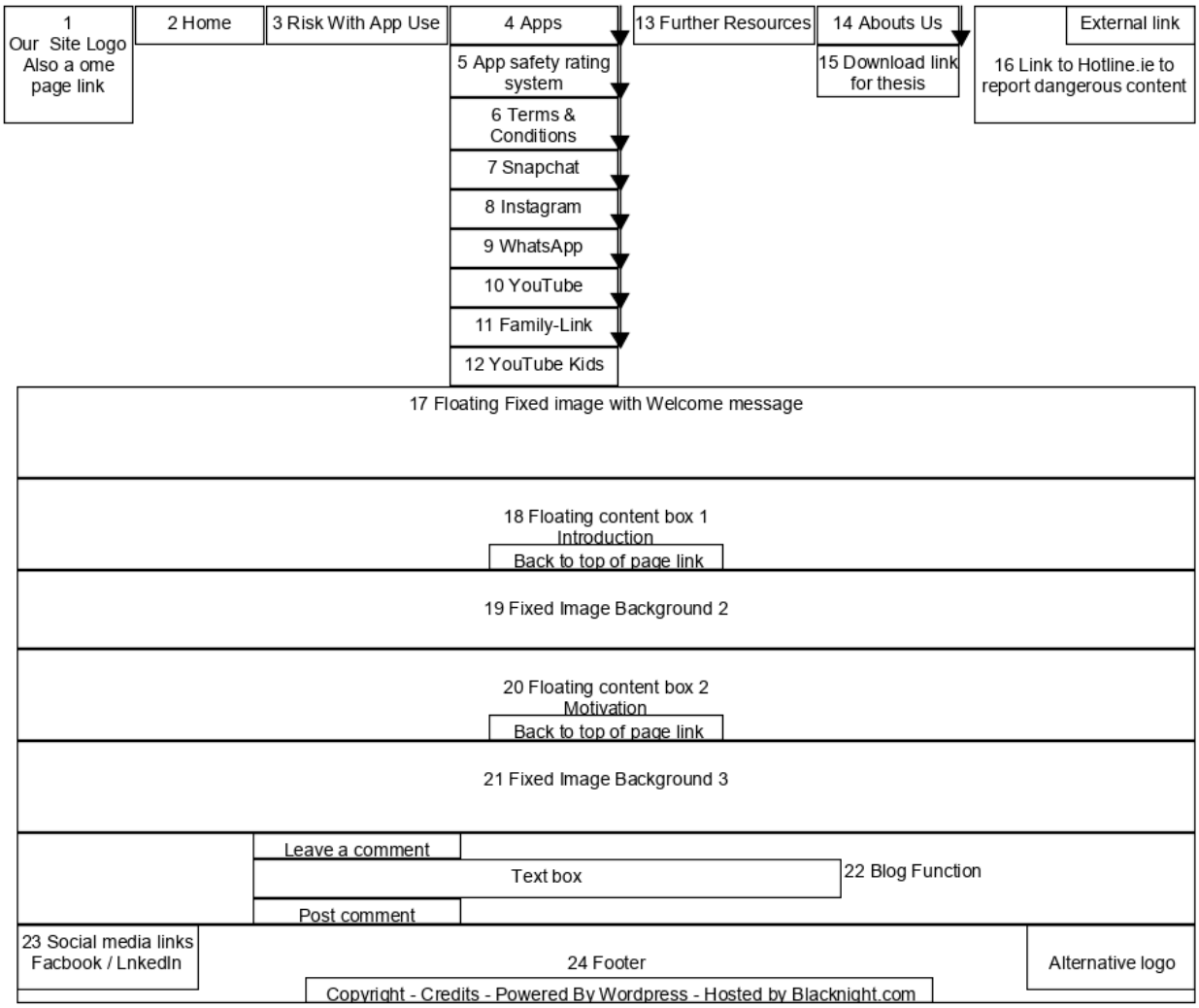


Page Legend:
1: Our service's logo – Also a home page link 2: Home page Link 3: Link to Risk with App Use
4: Link to Apps 5: Sub Link to App safety rating system 6: Sub link to Terms & Conditions
7: Sub link to Snapchat 8: Sub link to Instagram 9: Sub link to WhatsApp 10: Sub link to YouTube
11: Sub link to Family-link 12: Sub link to YouTube Kids 13: Link to further resources
14: Link to About us page 15: Sub link to Download our research thesis 16: External link to Hotline.ie's report illegal content link 17: Floating image with welcome text 17: page content
19: Fixed image 20: page content continued 21: Fixed image 22: Search function
23: Link to our service's social media 24: Page footer, Copyright section (link to credits included)

Template for all blog pages

All pages which permit blog feedback will follow the following template. Content will of curse vary and the number of sections will also vary. But the template for the following pages will maintained:

- App safety rating system
- Terms & conditions
- Risks associated with App use
- YouTube Kids
- YouTube
- WhatsApp
- Snapchat
- Instagram
- Family-link



Page Legend:
1: Our service's logo – Also a home page link 2: Home page Link 3: Link to Risk with App Use
4: Link to Apps 5: Sub Link to App safety rating system 6: Sub link to Terms & Conditions
7: Sub link to Snapchat 8: Sub link to Instagram 9: Sub link to WhatsApp 10: Sub link to YouTube
11: Sub link to Family-link 12: Sub link to YouTube Kids 13: Link to further resources
14: Link to About us page 15: Sub link to Download our research thesis 16: External link to Hotline.ie's report illegal content link 17: Floating image with welcome text 17: page content
19: Fixed image 20: page content continued 21: Fixed image 22: Blog Function
23: Link to our service's social media 24: Page footer, Copyright section (link to credits included)

12.4 Use Test Case for Our Website

To test the usability, presentation accessibility and overall functionality of our website, we designed a custom survey to be issued to selected users who volunteered to test our website for us. This survey was once again conducted via SurveyMonkey.com. We selected primarily parents to test the service as we felt this would be the largest group of users to benefit from our service and therefore would provide the most relevant.

In order to gather feedback however, we must wait until our service has gone live. For this reason, we shall document our use test case survey prior to launch. following up on any changes which may need to implement will be future work. Should the timeframe of the project allow it, we shall document all feedback and implement any changes, if any, user felt were required to improve upon our service.
Our use test case questions were as follows:

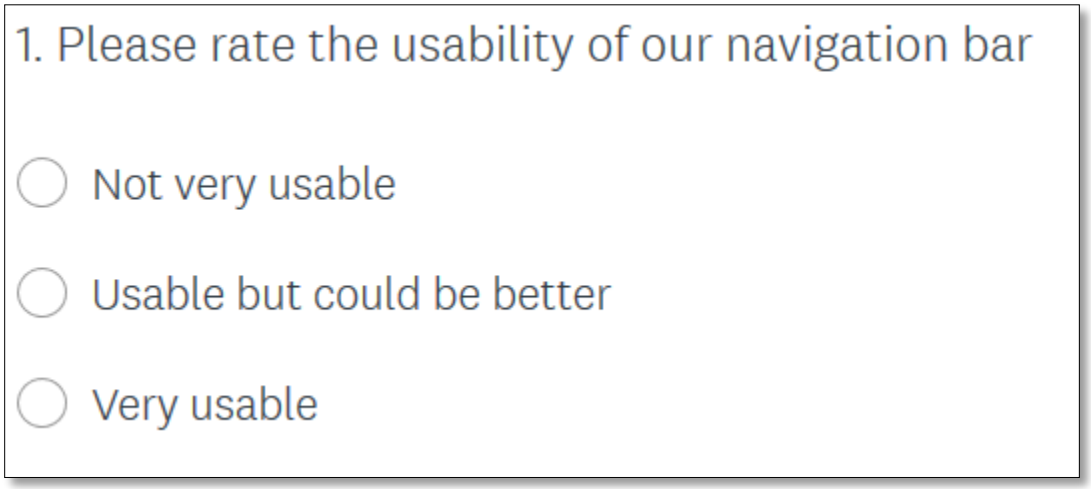


Figure 279 The first feedback question in our website use test case survey.

2. Please rate the accessibility of our content

- ◯ Very difficult to access
- ◯ Accessible but could be easier
- ◯ Easily Accessible

Figure 280 The second feedback question from our website use test case survey.

3. Please rate how navigable you found each individual page

	Introduction / Home page	Risks with App use	Apps	App safety rating system	Terms and Conditions	Snapchat	Instagram	WhatsApp	YouTube	Family-Link	YouTube kids
Not very navigable	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯
Navigable but could be better	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯
Easily navigable	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯	◯

Optional Feedback (if you found the pages not very navigable how would you suggest improving the navigability)

Figure 281 The third feedback question from our website use test case survey.

4. Please rate the presentably of the basic layout, including backgrounds style, fonts, color scheme of our site

- ◯ Very Bad
- ◯ Bad
- ◯ Acceptable
- ◯ Good
- ◯ Very good

Figure 282 The fourth feedback question from our website use test case survey.

5. • Should you have special needs such as text to speech for the visually impaired or a user with Dyslexia, please state any functionality the site might need to make it more user friendly and accessible for your use. We aim to be an inclusive service and wish to leave no user behind

Figure 283 The fifth feedback question from our websites use test case survey.

6. Please rate the usefulness of the blog function and the likelihood that you would use it to comment or ask questions

- Not very useful
- Useful
- Very Useful

Figure 284 The sixth feedback question from our website use test case survey.

7. Please rate the difficulty of implementing the guides offered up by our website

- Very difficult
- difficult
- not very difficult
- Easy
- Very easy

Figure 285 The seventh feedback question from our website use test case survey.

8. Our site strives to be GDPR compliant and to request only the most minimal amount of information and to store the minimal amount of data from its visitors. To be as open as possible we have provided a cookie notification and a data disclaimer for our blog post. We do not require user account creation and we only collect analytical data. Are you, the user, comfortable that enough warning, as to our data collection policies, has been provided and that enough effort has been made to minimize and safeguard your data?

- No
- Yes

Figure 286 The eight-feedback question from our website use test case survey.

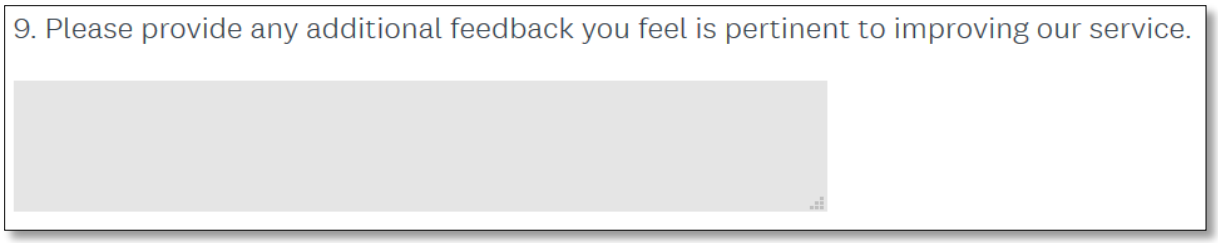


Figure 287 The ninth feedback question from our website use test case survey.

13.0 Conclusions

Returning to our research question, we must ask ourselves have we addressed the three principle topics within our research question. Does unfiltered access to online content via Apps present a risk to children, or indeed adults? The answer to this question is twofold within our feasibility study and our literature review. Our feasibility study highlights that the Irish government is aware that on-line content does indeed pose a risk particularly to young users. This is documented within their action plan as documented in our feasibility study (Section 6.0) (Department of Justice & Equality – Online Action Plan 2018). This action plan clearly recognizes the need for more services and subject material covering the area of online safety.

Further to answering this question, the sheer volume of resources currently provided also serves to highlight a clear indication that significant risks do exist in the area of online content. Hotline.ie (Hotline.ie 2019), as documented in our feasibility study (Section 6.0, Section 6.1), provides an anonymous form for reporting illegal content. As we can see in Section 8.6.1.1 figure 56, the figures and the facts surrounding the cases relating to the figures produce a startling picture of the grim reality of online content in Ireland. While the internet is largely a wonderful resource and a fantastic place for

children to explore their creativity, there does exist a murky underworld culture. The fact that the annual report released by Hotline.ie in 2017 (Hotline.ie Annual Report) shows that for the first time in eight years, child sexual abuse imagery was not traced back to Ireland, meaning that for the previous seven years it had been, shows that Ireland is a source of this kind of deeply concerning content.

Our case studies further serve to highlight this murky underworld. Operation Ketch III (An Garda Síochána 2018) highlights the scale of content that is out there. In this one series of raids an estimated 70,000 images of child sexual abuse were recovered while a further 150,000 went unrecovered. This suggests that in total, during this one series of raids, almost a quarter of a million were found to have existed. And yet this series of raids led to only one arrest. This suggests that one paedophile can generate or possess a vast library of child sexual abuse imagery.

In our second case study as documented by Anne Lucey (Lucey A. 2017) in section 8.6.1.2, we covered the case of a Canadian national who befriended a young Irish girl (14 years of age) for the purposes of grooming. As documented in this section, this man managed to convince this child to have intimate relations with him. He travelled to Ireland several times to have intimate relations with the young victim. This case is truly horrific and serves to highlight the very real risks that exist in the real world outside of the digital realm.

Here we have a grown man traveling thousands of miles to have to have intimate relations with a minor, which serves to show far beyond the grim prospect of imagery or digital content the risks relating to unfiltered online access via apps can, and in the worst-case scenario will, spill over into the real world and have very real consequences.

The annual CyberSafeIreland report (CyberSafeIreland 2018) covering 2018 documents that 68% of children between the ages 8 and 13 owned a smartphone. The report also indicates that 70% of this age range of children also use social media. Furthermore, 32% of children talk to strangers online per week with 18% conversing with strangers each day. Overall, 62% of teachers reported online related incidents regarding their pupils. 30% of children reported speaking to a parent regarding online safety within the last year, 24% within the last month and 30% had rarely spoken to parent suggesting they had at some point. But outside of the one-year range.

Of immediate concern was the age group of 8 to 9 years of age, with 27% of this age group reporting having never spoken to parents about online safety. This is of concern since it is estimated that roughly 50% of this age group are regularly online and using some form of social media. What the culmination of this data shows, is that children are exposed to both strangers and online content in an unfiltered manner.

We feel that the body of evidence presented in this report and as summarized here, definitively proves that the answer to the question: 'Does unfiltered on-line access to on-line content via Apps present a risk to children, or indeed adults?' is most definitely yes. A grave risk is posed by unfiltered access to online content via apps.

The next topic posed by our research question is: 'Are there adequate resources available, presented in a convenient user-friendly manner which enable a relatively novice user to implement procedures or settings that would reduce any risks posed by unfiltered on-line access to on-line content via Apps.'. This topic is also addressed via our feasibility study. In conducting our feasibility study, we sought to find resources recognized by the Irish government and major institutions such as charities that offer or provide services covering the area of online safety. We found that there are only five resources available that are recognized by the Irish government which are as follows: Hotline.ie, BeSafeOnline, Webwise.ie, Childline and NPC Primary. One noteworthy organization outside of the governments recommendations is the organization known as CyberSafeIreland which is Ireland's leading online charity relating to online safety.

Hotline.ie (Section 6.1) is a fantastic service which provides the ability to anonymously report content which users may believe to be illegal and provides further services relating to dealing with online safety and online content. However, in the area specifically of online safety the only content provided directly on the website which deals with reducing the risks involved with unfiltered access to online content is a list of parental control filtering apps. While these apps serve a useful function in securing a device they do pose a further question. If a filtering app is installed, and an app can be installed, does the filtering app provide any further security regarding in app settings with the app that is allowed to be installed. The answer to this question is no, most filtering apps do not provide this service. Therefore, once an app is installed, any inherent risks associated with that app are presented again. This only addresses the issue halfway. While an app is blocked you are protected from any inherent risks associated with it, however once an app is allowed to be installed, the filtering app provides no security and no reduction in visibility, this can only be done from within the App's settings.

BeSafeOnline (Section 6.2) is a portal service that hosts a library of links to services and resources provided under the umbrella of the governments BeSafeOnline service. However, no direct content is provided via the BeSafeOnline service.

Webwise.ie (Section 6.3) (Webwise.ie 2019) is perhaps the most well-rounded resource offered up by the Irish government. It provides a wealth of documentation, advice, tips, guides and media covering all areas relating to online safety. Furthermore, Webwise.ie is the host of the Internet Safety Day as documented in section 6.0. They also offer resources such as BeInCtrl which is a government backed initiative aimed at tackling the risks associated with online activity. They also have an anti-bullying initiative called UP2US which aims to tackle issues in schools to do with bullying. The focus of the area we propose to cover is specifically in app settings. Webwise.ie does attack this area however not in the user-friendly or in-depth manner we deem appropriate. As seen in sections 6.4 and 6.5 we felt that the specific area of optimizing an App's settings can be improved upon due to the lack of a full breakdown of the most popular App's settings.

For example, in section 6.4, while addressing the issue of GPRS settings in WhatsApp, the dangers associated with this feature are not mentioned and the aim is to highlight how to turn on this feature. This is in our opinion, a reduction in security. The failure to address both risks and counter measures to those risks is consistent throughout the App content coverage on the Webwise.ie platform. This is a rather significant blemish on an otherwise thoroughly useful platform, this is the specific area we aim to address.

The ISPCC serves a critical role in helping both children and parents address and attempt to prevent harm both physical and mental to children. While their website does offer some tips and advice centred around online activity it is not in depth and does not go into detail about the use of apps and optimizing their settings to secure an account in an online world.

The NPC primary is like Webwise.ie but focuses in face to face training offering courses centred around online safety. Its online resources are extremely limited.

CyberSafeIreland is Irelands leading internet safety charity. Every year they gather information and generate a report pertaining to children's online activity and the risks associated with it. Despite this report being a great source of data, gathered from schools ongoing yearly surveys, the other resources on the website are lacking. The website offers tips and resources but primarily in the form of links to support pages of Apps.

Our research during our investigation into each of these Apps shows that while many sources of resources do exist which tackle the issue of online risks, only one of the provided sources covers the specific area of online security and the reduction of the risks via in App settings. Therefore, the answer to the question' Are there adequate resources available, presented in a convenient user-friendly manner which enable a relatively novice user to implement procedures or settings that would reduce any risks posed by unfiltered on-line access to on-line content via Apps.' must be no as the coverage of the specific area of reducing the risks are negligible and this is the area we believe our service has addressed.

The final aspect to our research question is 'Is there a demand for said resources?'. According to the Progress Report on the Action Plan for Online Safety 2018 by the Department of Justice & Equality (Department of Justice & Equality – Progress Report on Action Plan for Online Safety 2018) [Accessed March 2019] the Irish government plans to create more resources for online safety as shown in section 6.0. "We will work with online platforms in Ireland to advance online safety measures." This shows that the Irish government believes there is a need for more resources relating to online safety.

In addition to this, according to the survey we conducted in our area (n = 100) we found that 28% of our participants felt their selected apps did not have clear and easy to understand security features with a further 33% not knowing about the settings at all. This shows 61% of our participants require more information which as we have shown, is currently not available.

Further to this point the annual CyberSafeIreland report (CyberSafeIreland 2018) covering 2018 documents that having providing information sessions covering online safety, 53.1% of parents felt very confident, 41% felt confident and 6.3% felt a little confident that they could go home and apply the settings. What this highlight is that if information is accessible and easy to understand, parents themselves can implement safety precautions to help reduce the risks of online content via Apps. This shows that there is a clear demand for such services. With these points in mind, the answer to the question 'Is there a demand for said resources?" is unequivocally yes.

With relation to our project goals our first goal was to answer the research question. Having done this, we asked ourselves, do we possess the skills necessary to fulfil the need to provide information required to reduce the risks associated with app use. We feel that we have fulfilled our goal in this area due to the fact that we not only performed an in-depth analysis of each app with regard to its security settings as shown in section 11.0, but we also provided an easy-to-access easy-to-understand platform to display this information which took the form of a website (Safeappuse.ie 2019).

As discussed in our research question we have determined that a risk does exist surrounding children's unfiltered access to online material via Apps, therefore our first research goal is reached.

The next research goal we set for ourselves was to design a survey specifically aimed at parents and children to confirm if the information provided by the CyberSafeIreland annual report 2018 was still relevant and to see if users felt there were security concerns surrounding Apps that concerned their children using the platform and if they are satisfied or aware of the settings available. Using Survey Monkey, we constructed a survey and conducted the survey in our area with a sample size of 100 (Section 8.2) this survey supported the findings of the CyberSafeIreland report (Section 8.3) as well as highlighting parents' concerns regarding App use. Beyond the original scope of this survey it also provided a wealth of useful information as documented in Section 8.3 which helped in other areas of our research including App selection, narrowing our platform's focus, development of our App Safety Rating System and additional concerns parents may have regarding security. With this research goal complete we moved on to the next.

We briefly discussed the use of VPN's. As it transpired during the course of our research it was discovered a VPN was required in the setup of the Google Family-Link App. This being the case, this afforded us the opportunity to cover the concerns, fears and general misconceptions regarding VPN's which also allowed us to add in an extra layer of security should users wish to use it as shown in section 10.0.

As previously highlighted here in the conclusions the case study was conducted as shown in section 8.6 and served a pivotal role in providing project justification and in specifically highlighting some of the more serious concerns regarding unfiltered online content accessed via Apps.

Using the data from our case study combined with the experience we have gained during our studies in Digital Forensics and Cyber Security, we developed an App safety rating system that awards points to an App having attributes or features that make it safer to use.

We researched the selected Apps in detail reviewing the terms and conditions along with privacy policies to see how person data was used or stored by the App. We then investigated and reviewed the security settings and features provided by the app and recommend the safest configuration possible to ensure a user's online visibility is reduced making it harder for marketing agencies or product manufacturers to gain access to the user's data, while also reducing the potential for malicious users to abuse the information that may be available.

We designed a web-base WordPress blog to provide our content in a user-friendly and easy to understand way. We wish to make the website secure by adding an SSL certificate in the future however this was not in our research goals. We created a simple introduction page which covered the basic content a user can expect to find on the service including the risks related to unfiltered app use, a distilled version of the terms and conditions for the apps which aims to highlight the import of content which may be missed if a user elected to overlook the terms and conditions is documented.

Also including of course is the main body of content which covers the in-app features and settings as well as tutorials on how to reduce the risks. The terms and conditions, as well as each individual app are given a separate page. The introduction page also included our motivations which describe why we felt the service was necessary. Each of these pages also includes a blog forum which allows users to give feedback and make requests via a direct on page comment form which must then be approved by a moderator.

A simple search function was provided to facilitate the ability to search the site from the home page. This is purely a quality of life addition. Where a page is considered to be extensively long, links are provided regularly to make it easier to return to the top of the page for website navigate. Also, within each blog page, links are provided to allow users to navigate to the previous as well as the next post.

GDPR integrity was maintained as no data which is not volunteered is collected. That data which is collected is purely cookie related data and is no way datamined. A data sharing disclaimer is included to cover the blog section as a well as a general cookie warning, giving users ample opportunity to leave the site before any data is entered. The maximum data that would be required would be a name to which we can respond, and an optional email should the user wish to provide it.

The home page also includes a direct link to Hotline.ie's form which allow the anonymous reporting of illegal or inappropriate content. Each page also includes social media pages created to accompany the website. While this was not documented within the scope of the website this feature was added purely for scalability should we decide to continue developing this service in the future. Our site also includes a page dedicated to informing the users on who made the site and what their knowledge and experience is. Each of our group members provided a brief description of their personal experience in the world of Computing and specifically cyber security and digital forensics. We also provided a facility where users may contact individual members discreetly, directly via email and LinkedIn. This was provided for those users who may have serious questions but wish to maintain their anonymity.

As this blog was designed to complement other services who do an amazing job of highlighting the many risks associated with unfiltered access to online content via Apps or providing services to deal with illegal content or some form of assistance, rather than compete with them, we created a simple page which lists the main resources with external links to them as recommended by the Department of Justice and Equality Cybercrime division (Department of Justice & Equality 2019).

Lastly, we provided a directly link to our Thesis for those who would evaluate the research behind the content of the site. While the website itself was designed to display information as simply as possible the research behind the content was very in depth and thorough. This is far too much information to display on the page however we feel like the information could be very useful to users or even other students who may wish to study the research material. Therefore, the full thesis will be available to download directly from the site.

Reflecting on our primary research outcomes we feel that we have provided ample coverage of the in-App settings such that users, particularly adults, will be able to make informed decisions on App use. Both in terms of understanding why a child may wish to use an App and the risks associated with it. This allows users who are less aware of modern devices or applications to way up the features of an App verses the risks associated with that App. Should the user elect to install an App the depth of coverage for the in-App settings allows the user to provide the appropriate level of security he or she feels is appropriate to the situation, from the most stringent and restrictive of options to the most permissive.

While ultimately the use of an app, or the decisions regarding how restrictive or permissive the settings are applied is ultimately down to the user. We have provided an App Safety Rating Score for each App based off our best practice recommendations being implemented. We feel that this further allows parents to make more informed decisions and should incentivize those users who elect to install what we deem to be an unsafe App to follow our best practice recommendations. For example, Instagram with a score of five is considered to be an unsafe App for any user but particularly where children are concerned. Therefore, we feel this low score incentivizes users to apply the most restrictive settings as per our best practice guide to balance the features of the app and the risks associated with the app, to gain the best user experience while employing the best security practices to reduce user visibility and online footprint.

While it was very difficult to show the results of the best practice recommendation in its entirety for each App, as the use of an App and the individual settings applied are so case specific to each individual user and their setting preferences it would be impossible to document all the possibilities within the scope of this project. What we could do however, was to implement Google Analytics on our website. Having gone live with our website we attempted promote the website to attract users to the website. Having generated some activity on the website we used the Google Analytics to document website traffic such as page views and new versus returning users.

With our website now completed and live, we took a moment to reflect on the journey this project led us on. It was both intriguing and concerning to the group as we justified the demand and feasibility of our project by answering the research questions and goals. While the area of online safety is so well documented this specific niche section which is so important to the security of users particularly children was so inadequately documented with almost no resources available covering in App settings. This drove us to be as clear and concise in developing our survey as we would essentially be one of the first groups to cover this area in such detail.

With our report completed, we felt we have conclusively covered the subject of the risks associated with App use and how to reduce or mitigate these risks with the proper application of in-App settings. We felt that in covering this hole in the current research we have learned a great deal and we felt we had a great responsibility to properly present this information on our website in the hopes that users would find this information useful and it would help to provide safety to children regarding online App use.

As the launch of the website approached, we felt that we had achieved this goal, our website is functional yet simple. We have strived to maintain a high level of usability through the application of good UI/UX methodology. The information contained within the website is concise, easy to understand, easy to access and fulfils our wish to provide a greater level of security to children regarding online App use. The skills we gained in the undertaking of producing this report and the website are skills that we will take forward into our working life.

As the final step in our project beyond our conclusions, we endeavoured to document all future work that which would be completed and which we felt should be completed however lies beyond the scope of our project goals.

13.1 Future Work

13.1.1 Test Case Demonstration of App

Having completed the main body of our report, we endeavoured to document a use test case of one the App which the research of both CyberSafeIreland and our own group highlighted as being the most popular app currently in Ireland, YouTube.

To facilitate this demonstration of the effects of our guide when partially or fully implemented, several test accounts where create both in google and YouTube. 3 of these accounts were used to highlight the following:

1. Unfilteredyt1: This account demonstrates no implementation of the guide.
2. SemiFilteredYt1: This account demonstrates a partial implementation of the guide with only YouTubes Internal settings
3. filteredYt1: This account demonstrates the full implementation of both YouTube and Google settings as per the guide.

Each of these test Apps has the same user name: Joe Bloggs. And is considering to be 16 years of age as any younger would demand the use of a parental account to sign off on the terms and conditions. A further account was created to act as a malicious user: johndoeyt740. The name on the malicious account name is John Doe and the age was set at 21.

For our demonstration our main goal will be to demonstrate 3 things relating to the risks associated with inappropriate content via the YouTube App.

1. Inappropriate Content unfiltered versus filtered via settings: do our recommendations reduce access to inappropriate content.
2. Malicious Users: Can we restrict the ability for Malicious or abusive users to contact young users via comments or friend requests.
3. Can we reduce the overall visibility, footprint and potential data leakage of a user's account by altering YouTube and/or google settings?

Ethical Framework Approach to risks

Inappropriate Content:
When approaching the issue of inappropriate content, we viewed this issue from three ethical framework perspectives: Lawful, Freedom and Safety. Regarding content uploaded to any hosting service we must consider the minimum age restrictions of users using the site as specified by the terms and conditions of the use of such sites. Any user accessing any content on such hosting sites who falls outside of the minimum age restrictions creates a legal issue because they shouldn't be accessing the service at all.

Regarding inappropriate content we must now approach it from within the freedom framework perspective. It is not for us to decide what is legal or illegal to host, nor is it for us to decide what content creator is free to upload. Users are free to post anything they wish if it does not breach YouTube's terms and conditions, however conversely, users are also free to determine what they consider to be inappropriate content for themselves or their children.

Therefore, from the perspective of a parent any content may be deemed inappropriate. Therefore, we aim to provide a filter that we will provide an adequate level of protection.

We must now view inappropriate content from within the safety framework. If the content in question hosted on the services potentially poses both mental and physical risks to its users. Those users or parents of their users should be able to filter that content to remove risk. For example, if a parent of a user found that their child was being bullied in the comment section of YouTube videos this would be harmful for the child in question. This bullying presents a mental safety risk to the user. YouTube does provide settings to disable comments and block user which would aid in the safety of children using their app however YouTube has these safety options disabled by default.

Malicious Users:

Malicious users, when evaluated from an overall ethical framework could again fall into the following categories: Legal, Freedom and Safety. From the perspective of a legal framework there is no doubt that there is a question of legality surrounding malicious users. While some users may seek to bully other users, there are also other malicious users that may seek to victimize other users in attempts to phish information. This information may be used to gain access to accounts which may lead to actual theft. Lastly, we must also acknowledge the potential risks regarding predators wishing to groom young users or worse. Users and parents of users will naturally be seeking protection from these malicious users.

Malicious users when viewed from the perspective of a freedom framework are clearer cut. Obviously malicious users do not have the freedom to abuse the comment section of any app, or to inappropriately contact any user, particularly young children for the purposes of solicitation and exploitation. If viewed from the other side of the freedom framework users and parents do have the freedom to exclude these malicious users from their user experience.

Malicious users when viewed from the perspective of a safety framework pose a very real threat to the safety of anyone using the platform. The obvious risks to the safety of its users would be the potential for phishing which as mentioned before could lead to potential theft. There is also a potential for mental anguish caused by bullying via the comment section with could even potentially lead to self-harm. And worst of all is the potential safety risks surrounding predators and groom with the potential of online grooming extending into contact in the real world between these children and predators online.

Data Leakage:

Data leakage also falls into the following categories about ethical frameworks: Legal, Freedom and Safety. We cannot view this from a legal perspective because the platforms in question specifically require the users to accept the terms and conditions which state that although they will attempt to prevent any data leakage if such a thing should occur you have already accepted that you cannot pursue it legally.

When viewed from the point of freedom, companies are allowed to gather and collect your data however users also have the freedom to also opt out of this data collection to reduce the possibility of such data being leaked. While google do provide options for this, these settings are buried deep within the google user settings and are not easily accessible if the user is not aware of them. Therefore, we felt it was very important to provide information and guides on these settings to reduce the amount or likely hood of data being leaked.

When viewed from the perspective of safety, it could be argued that there is a small safety risk surrounding the leaking of data, as security students we are well aware of the ability to enumerate accounts based off small amounts of leaked data and the existence of tools to datamined such data. While this risk may be considered small in comparison to legal and freedom framework considerations, safety cannot be ignored. Therefore, we must provide our guides to detail how to prevent such risks.

Inappropriate Content

So, for our step we shall log into our first test account and search for inappropriate content. We shall do a simple word search using the word "porn" and see if we get inappropriate content. And in this case, we do indeed gain to inappropriate content as seen below.

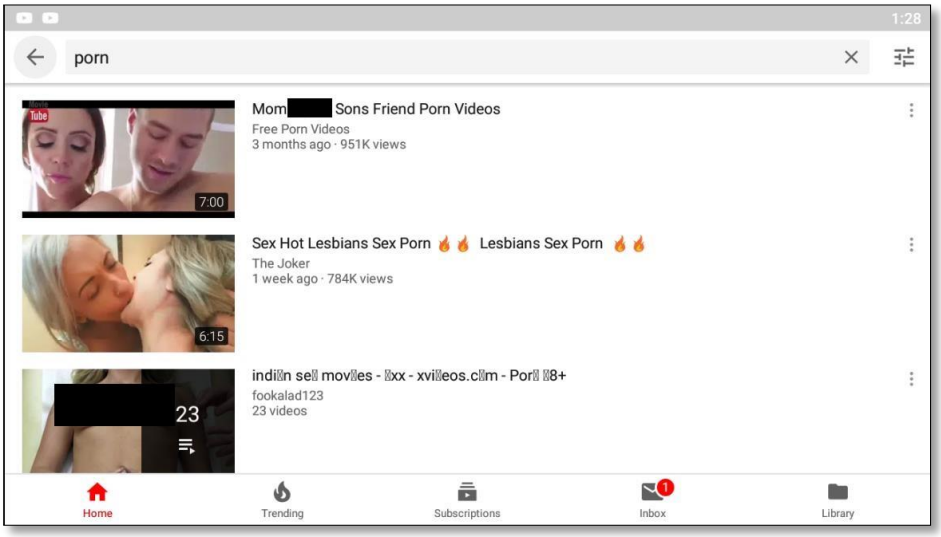


Figure 288 Unfiltered access to inappropriate content

Next, we shall attempt to remove this access by logging into our second semi filtered account and applying restricted mode reduce the ease of access to this inappropriate content. This does alter the results of the word search.

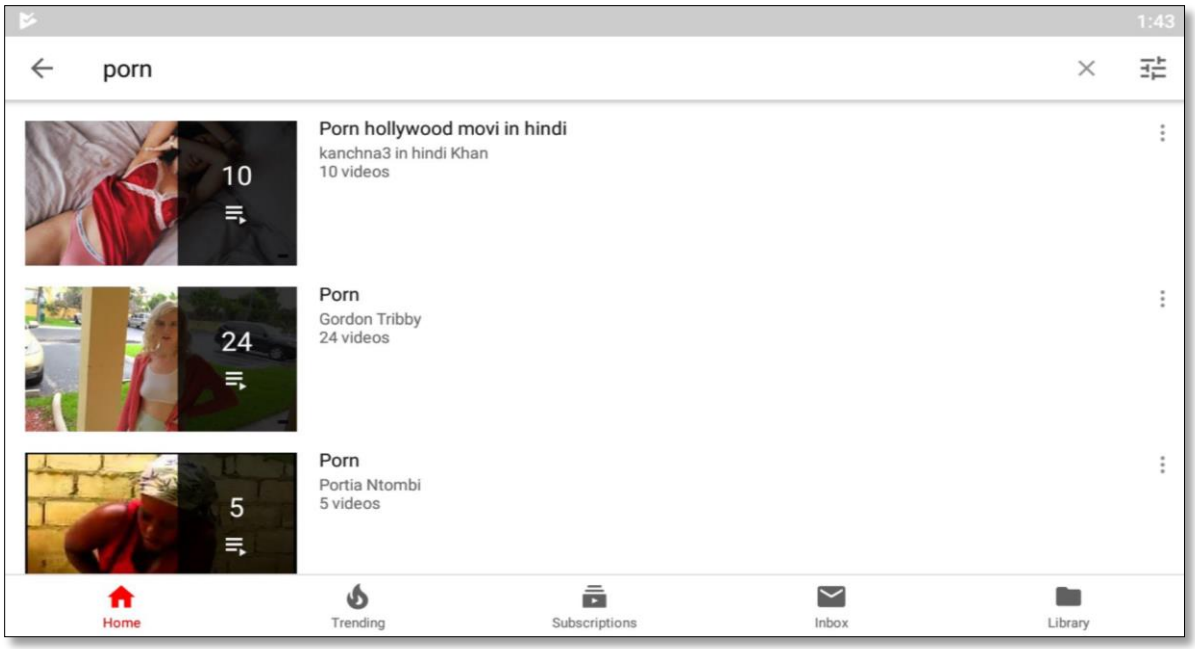


Figure 289 We see a different set of search results.

Obviously, we can see that even just the thumbnails in the first search are very inappropriate for young children. Indeed, we considered the second set of results also inappropriate although we feel that the filter is having an obvious affect and reducing the inappropriateness of the thumbnails. The content itself. While none of this content is true pornographic material, the content is far more risqué click bait in the first search and less inappropriate click bait in the second search.

So the effect here is that access to inappropriate content is indeed reduced although the restricted mode is not perfect. Some level of inappropriate content can still be reached due the nature of the algorithms used by YouTube and the diverse nature of the content uploaded.

The final thing to note regarding inappropriate content is that the comment section of YouTube can quite often be a very toxic place. This is a known issue with social media in general which we have touched upon in our report. Our first test account being unfiltered has no restrictions regarding this inappropriate content. The second test account however, having restricted mode enabled, is prevented from viewing general comments precluding the possibility of becoming embroiled in this toxic environment for all content not posted to the test users account, as seen below.

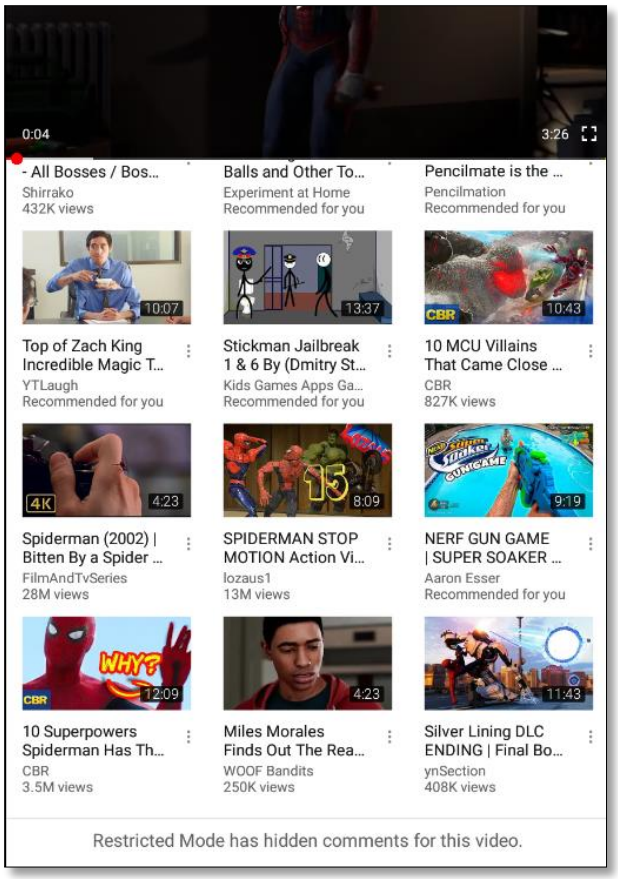


Figure 290 Here we see comments disabled via restricted mode for our second test account

There are however flaws in this increased filtering system. If the user were to post a video to their account, the video will by default be posted in public mode. This will bypass restricted mode, allowing comments to be placed by malicious users.

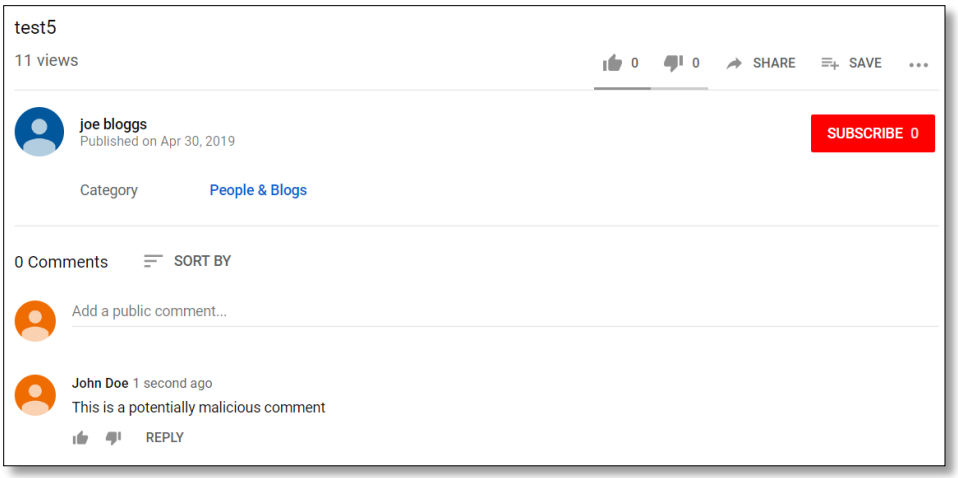


Figure 291 Here we see the public video posted to the second test account with restricted mode enabled, but a comment may still be placed.

This issue can be addressed by either ensuring that the child alters all videos to be posted as private. The child could also adjust each individual post to be public but have comments disabled, however this could easily be overlooked so we do not recommend this. or simply by not posting videos at all, which would be our groups recommendation. As we see, we have added several layers of protection, but the protections are not perfect.

Malicious Users

As far as methods for malicious users to reach out to young children go, the comment section is not the only way in which a malicious user can reach out to other users. There is a friend system in place in YouTube, however, uniquely, links must be generated and sent to the desired user. The user must click on this link and accept the friend request. These links can be sent via other social media platforms if the user has access to the desired users accounts outside of YouTube. This can also be done internally if the account which you are attempting to share a friend link with has content posted with comments enabled.

To reduce the likely hood of this, any malicious users can be blocked. This will prevent them from commenting on videos and messaging users directly if that user has previously been added as a friend.

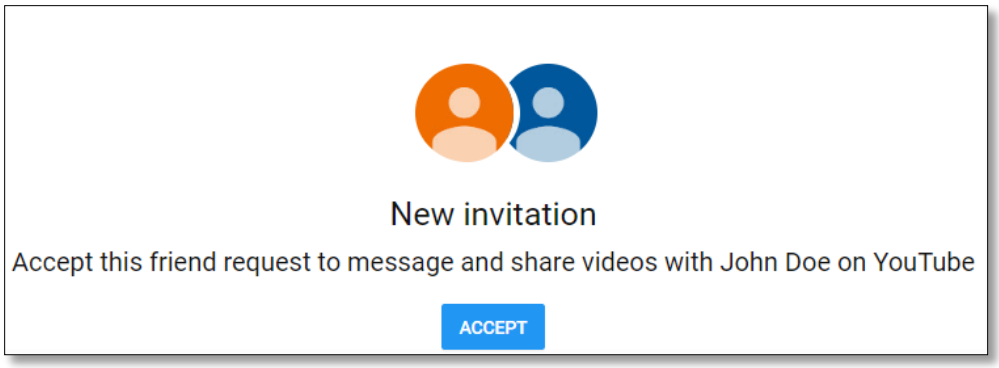


Figure 292 Here, we see a friend request sent via Facebook to our second test account from the malicious user account.

However, there are some tricky flaws to this block setting. It will not however prevent the user from sending a link via another platform. If the user clicked on this link sent by the malicious user, they will receive a warning telling them that accepting this link will remove the block. Therefore, it is conceivable that a child may accidentally remove any such blocks.

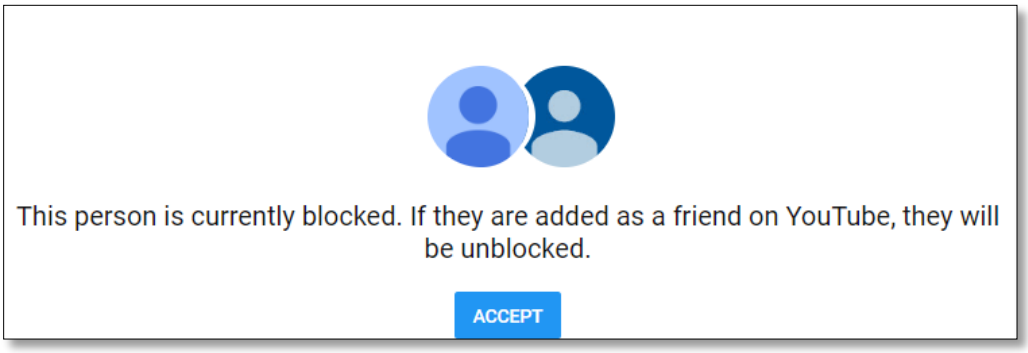


Figure 293 Here we see the blocked malicious user has sent a further request and our child has been warned that accepting this link will remove the block.

Reduce the overall Visibility, Footprint and Potential Data Leakage

To reduce potential data leakage, either by having your profile datamined through the use of open source intelligence-based tools, or to avoid simply having your likes and subscriptions tracked enabling users to potentially enumerate accounts on other platforms, we recommended disabling all google data sharing and tracking settings.

These includes:

- Web & App activity
- Location sharing and history
- Voice and Audio activity
- Device Information
- YouTube search and Watch history as well as
- Recommended ads and endorsements.

As can be seen below, Web & App activity, YouTube Search and watch history as well as shared add endorsements are all enabled by default. We changed these to off, ensuring that should any data leak, the minimum amount of data is leaked reducing the likelihood of any tools producing useable results. Naturally, if Google is prevented from gathering such data, the Users visibility and footprint are drastically reduced.

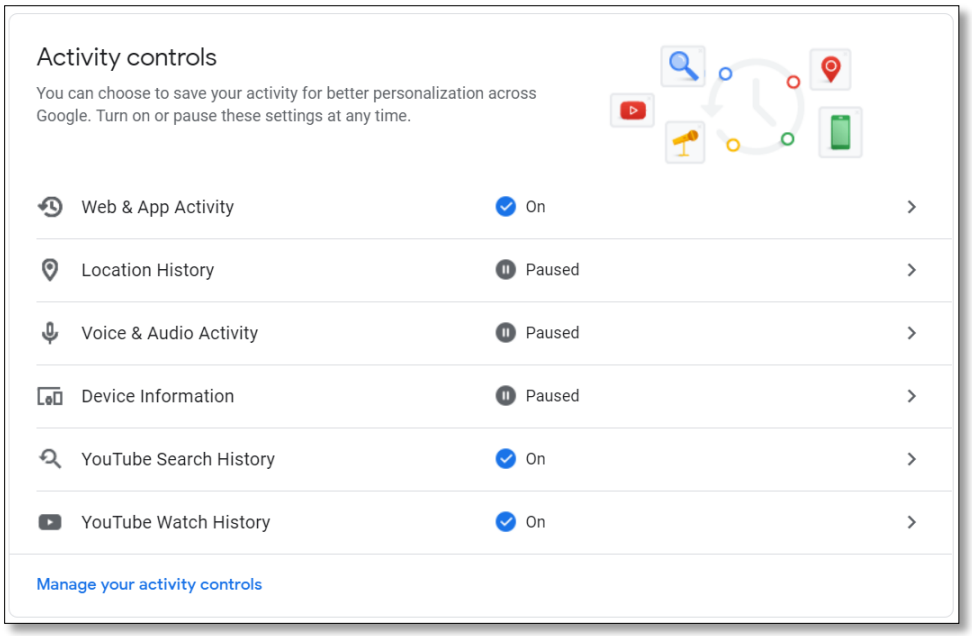


Figure 294 Here we can see the default arrangement of google data gathering settings. These we switch to off.

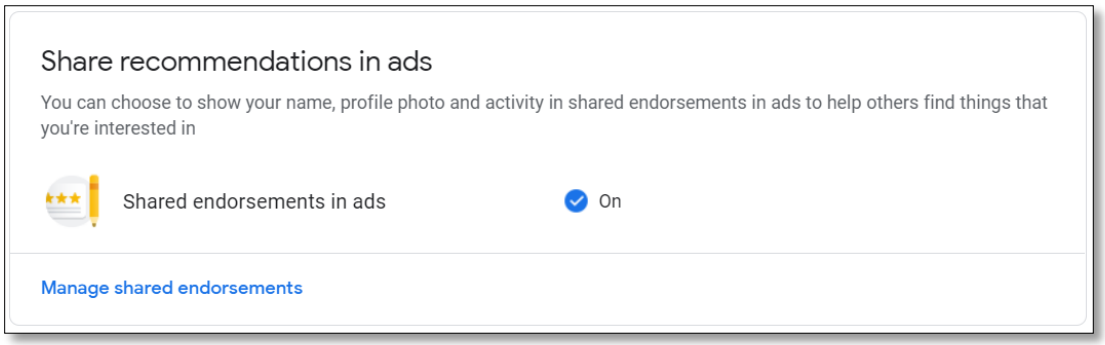


Figure 295 Here, we see googles shared endorsements setting is on be default. This was also tuned off.

Naturally documenting the difference of what is collected with settings enabled, versus what is collected with settings disabled, due to time constraints is beyond the scope of our project as it would require generating multiple sets of data and downloading over periods of time to compare data sets. This is simple beyond the time and scope of our project however, if should be obvious the impact these settings being disabled will have.

YouTube Fully Filtered

As we have demonstrated, our setting changes from our guide have resulted in significant filters relating to the risks associated with content being accessed via YouTube. However, we still feel that flaws exist even in these filters. So, while we have added various layers we shall continue as per our guide towards the maximum level of protections. This requires us to remove YouTube from the equation and move on to YouTube kids and Google Family-Link.

There are two main benefits from this aside from any settings we may apply in either of these Apps. Firstly, the comments are automatically disabled by default. And secondly, the content is already prefiltered to remove much of the possible inappropriate content.

We do recommend however, that the google settings be applied regardless of whether the user opts to accept any potential risks and use the main YouTube App, or adopt the fullest protections and go with YouTube kids & Google Family link.

YouTube Kids

Where YouTube, even fully filtered retains some flaws, YouTube Kids is more successful by tailoring their platform to a younger audience, and a result they put security on the forefront. YouTube Kids already comes with default content filtering features, like the filtering of your search ability in comparison to YouTube and the ability disable the ability to search feature entirely.

We set up YouTube kids as a parent, who would then set up a child account on the App, that they could use on their own device, as per our guide. When we were setting up the YouTube Kids App, we were asked to provide our year of birth to prove that we are in fact, old enough to set up this App.

Having set up this account, we had set up the settings on the App, as was laid out by our guide:

- Approval Content Only – This allows us to choose what types of content can be seen, further tailoring what content can be viewed on the platform. This in turn reduces the ability for inappropriate content to appear on the platform.

- Pause history – This allows us to prevent the app from suggesting videos related on the videos that we watch, be it on the main page, the suggested videos on other videos, or on the search bar. This reduces the ability of data leakage from occurring.

- Kid's Secret Code – This allows the kid to setup a secret code for their account, to keep the app safe from other children who might use the device.

- Search Function – This gives us the ability to allow or disallow the Search function on the App, which we have chosen to disable.

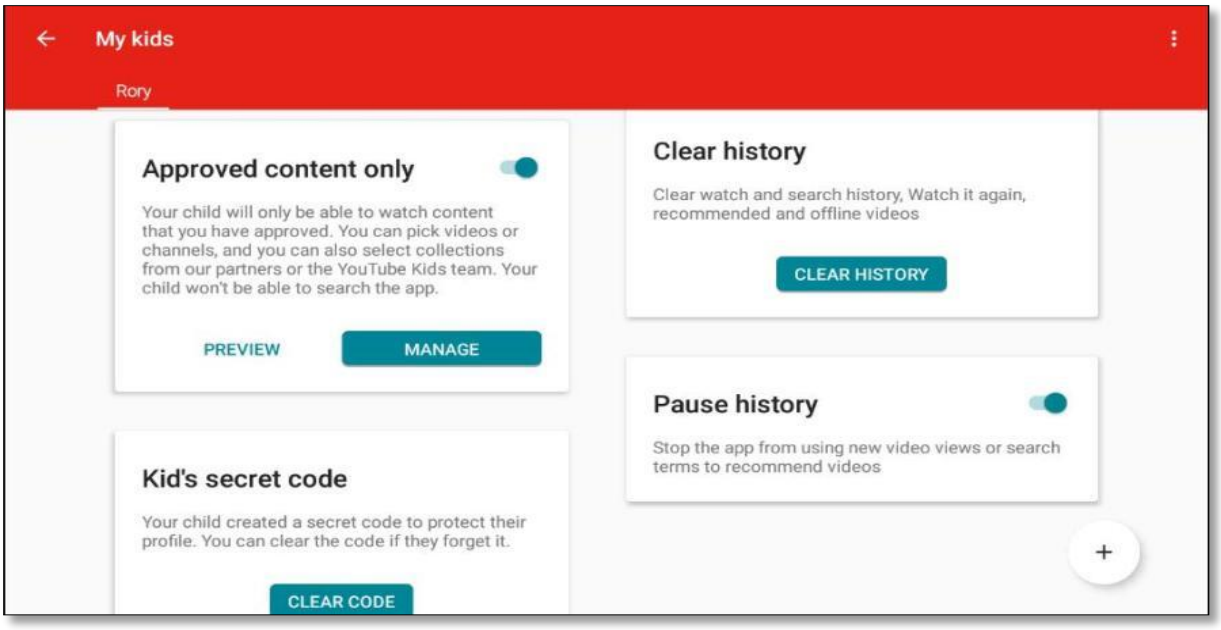


Figure 296 Parental options adjusted as per our guide.

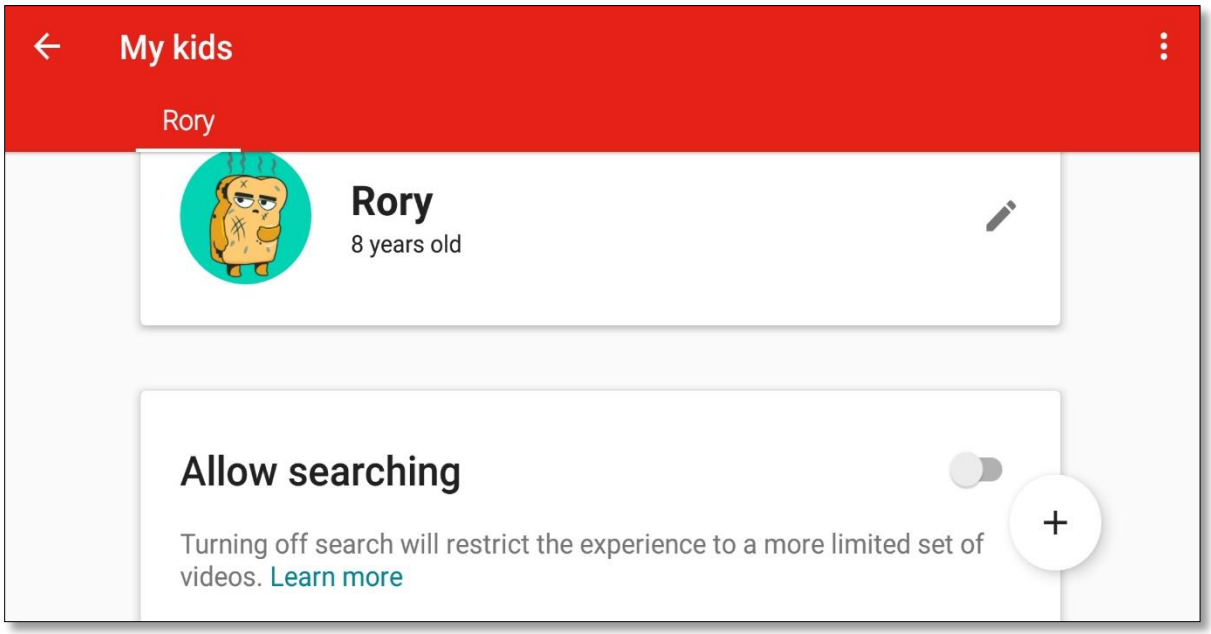


Figure 297 Parental options adjusted as per our guide.

Regarding dealing with malicious users. There is no feature on the platform for users to communicate with each other in any capacity. Therefore, no advance settings are needed to deal with malicious users due to the very nature of the App.

For dealing with inappropriate content, as previously shown, the app already pre-filters content and divides content into themes, as was covered in our report. The addition content of the Approval Content Only setting provides a furthering filtering option. The level of reduction of possible accessing of inappropriate content is drastically higher than with YouTube, which provides no prefiltering, and no secondary filtering options.

As far as data leakage is concerned, the addition of the pause feature setting is a great feature in regards in the reduction of possible data leakage, however, we do recommend the addition of the Google settings, as previously recommended in our report.

YouTube Kids is more secure with all these settings applied, compared to YouTube Kids without settings. Furthermore, this set up is also more secure then the default YouTube App. When it comes to the filtering of YouTube Kids, the content is filtered to prevent inappropriate content from coming through, which is a plus compared to the default YouTube App, which only filters based on age. The addition of the Approved Content Only serves to only enhance the filtering of inappropriate content.

While we do recommend, as with all apps, that the Google options should be adjusted, as previously shown. The addition of the pause history setting found on the YouTube Kids app serves to add an additional layer in the prevention of potential Data leakage. All in all, the use of YouTube kids over the default YouTube App has resulted in a significant decrease in the risk of inappropriate content, the possibility of encountering malicious users and the possibility of a data leakage.

YouTube kids with Family Link

Our first step in setting up the maximum protection is to sync up Family link, with our YouTube Kids App, which we have done. Having done this, we then set about optimizing the settings in family link. The first setting which we adjusted was the location settings. We've double checked the ability to add and remove users, install apps for unknown sources, and activate developer mode have been turned off. We had set up a screen lock of 0000 for demonstration purposes. We set the age restriction for Google play games to PEGI 7, Google Movies to PG, we restricted sexually explicit books and restrict music that is considered explicit by content providers. Google play purchases have been set to require approval on all content. We have also forbidden 3rd party apps, the sharing of google photos.

As previously mentioned, family link takes over particular settings from YouTube Kids, the settings affected by this are as followed:

- Search Function – This gives us the ability to allow or disallow the Search function on the App, which we have chosen to disable.
- Unblock Videos – This is a feature rather than a setting, so nothing has been adjusted.
- Activity Controls – This section contains the ability to disable search history and watch history remotely (this was previously controlled from within YouTube Kids), we have chosen to disable both of these features, as suggested in our guide.

With the addition of Family Link, we have gained the maximum level of protection achievable under our guide. The protections even go beyond the scope of the YouTube Kids App, giving us the ability to manage the following remotely:

- Manage Apps/Content: Block/Allow Apps to be installed
- Block Apps from Unknown sources and 3rd party Apps
- Filter all content in Google Chrome browser
- Apply age restriction for all features of the Google Services
- Monitor and manage all activity of the child's device and account remotely
- Set up and manage Screen times
- Manage YouTube Kids Search function remotely
- Block the recording of Search History and Watch History on the YouTube Kids App remotely

The maximum levels of protection is gained when YouTube Kids is used in favor of the YouTube App, in conjunction with Google Family Link. As previously mention, YouTube Kids gives us the ability to have prefiltered content on the App, as opposed to YouTube which only filters by age. Furthermore, YouTube Kids allows us to disable the search function. There are positives and negatives with the integration of Google Family Link and YouTube Kids. For Example, we have gained the ability to manage some of the settings like, enabling/disabling the search function and managing the account activity remotely. However, one drawback is that due to a glitch with the combination of these apps, we have lost the ability to filter the YouTube Kids content more with the Approval Content Only function, we feel that this is a small sacrifice compared to the benefits gained from having Family Link. As per our previous setup, commenting is disabled in YouTube Kids giving a comfortable level of peace of mind regarding the reduced likelihood of malicious users to contact the child. This manages both inappropriate content and malicious users.

As we have previously stated, we recommend applying the Google settings on the users Google account as stated above. Reduces the amount of data leaked should a data leak occur.

The addition of family link provides many benefits beyond the scope of the YouTube Kids App, the main benefit gained in regard to YouTube Kids is the ability to manage some settings remotely. However, this remote management functionality is extended to both device and account management in almost every area of usability the child is likely to enter. The addition to remotely block and allow Apps, Filter content on Google Chrome, Apply an age restrictions to all Google Services and Google Content, set up and manage all the activity of the child's account and device remotely and set up and manage screen times all provide a level of increased protection, security, future proofing and peace of mind for any child or parent that is both high and easily obtainable. We feel that this is the maximum level of security obtainable whilst still retaining the functionality of YouTube Kids.

14.0 Appendix

List of countries that make up the EU region

European region:- Andorra, Austria, Azores, Belgium, Bulgaria, Canary Islands, Channel Islands, Croatia, Czech Republic, Denmark, Estonia, Finland, France, French Guiana, Germany, Greece, Guadeloupe, Hungary, Iceland, Ireland, Isle of Man, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Madeira, Malta, Martinique, Mayotte, Monaco, Netherlands, Norway, Poland, Portugal, Republic of Cyprus, Réunion, Romania, San Marino, Saint Barthélemy, Saint-Martin, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, United Kingdom sovereign bases in Cyprus (Akrotiri and Dhekelia), and Vatican City.

Website Use test case survey feedback

Having completed our Website and going live we created a second survey to document the feedback of our use test case users as document above in our report. We selected 10 users to acquire feedback from anonymously ranging across a variety of users from parents to young adults. We sat with user as they explored the website and encouraged them to give real accurate feedback both positive and negative where ever they felt they had feedback to give. The results were as follows:

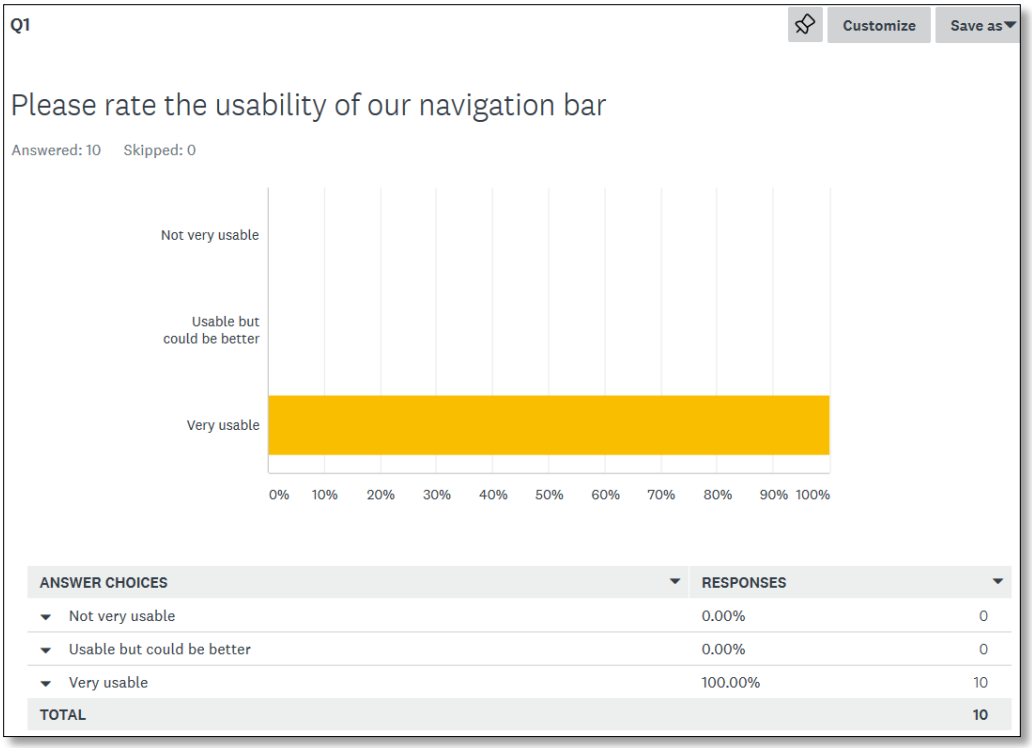
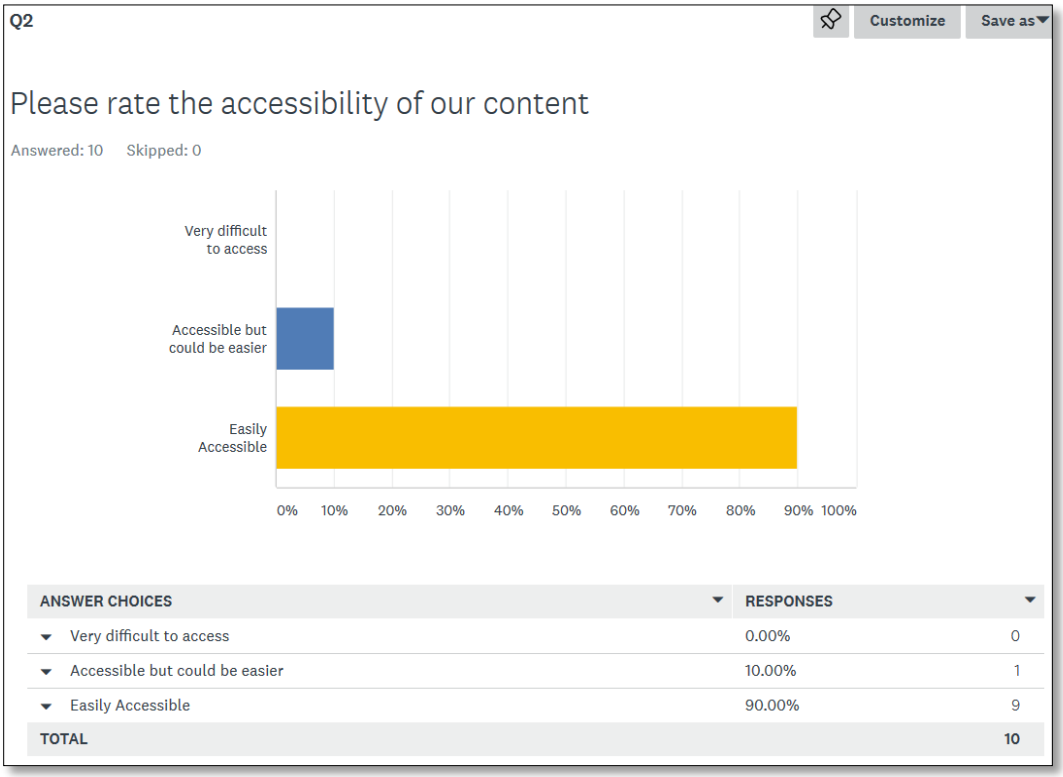


Figure 298 Here we see fully positive feedback regarding the usability of our navigation bar.

This first question was aimed at getting feedback regarding the usability of our navigation bar as this would lend a lot to the overall navigability of our service. The results show the feedback was overwhelmingly positive with 100% of survey participants describing the navigation bar as very usable.



ANSWER CHOICES	RESPONSES	
Very difficult to access	0.00%	0
Accessible but could be easier	10.00%	1
Easily Accessible	90.00%	9
TOTAL		10

Figure 299 Here we see the feedback regarding the accessibility of our content.

Question 2 aimed at gathering feedback regarding the accessibility of the content on our pages. While this question did result in overwhelming positive responses with 90% of survey participants describing the content as easily accessible, those responses did often come accompanied by a caveat. While users found the content accessible, they would have liked the content to broken up into smaller sections.

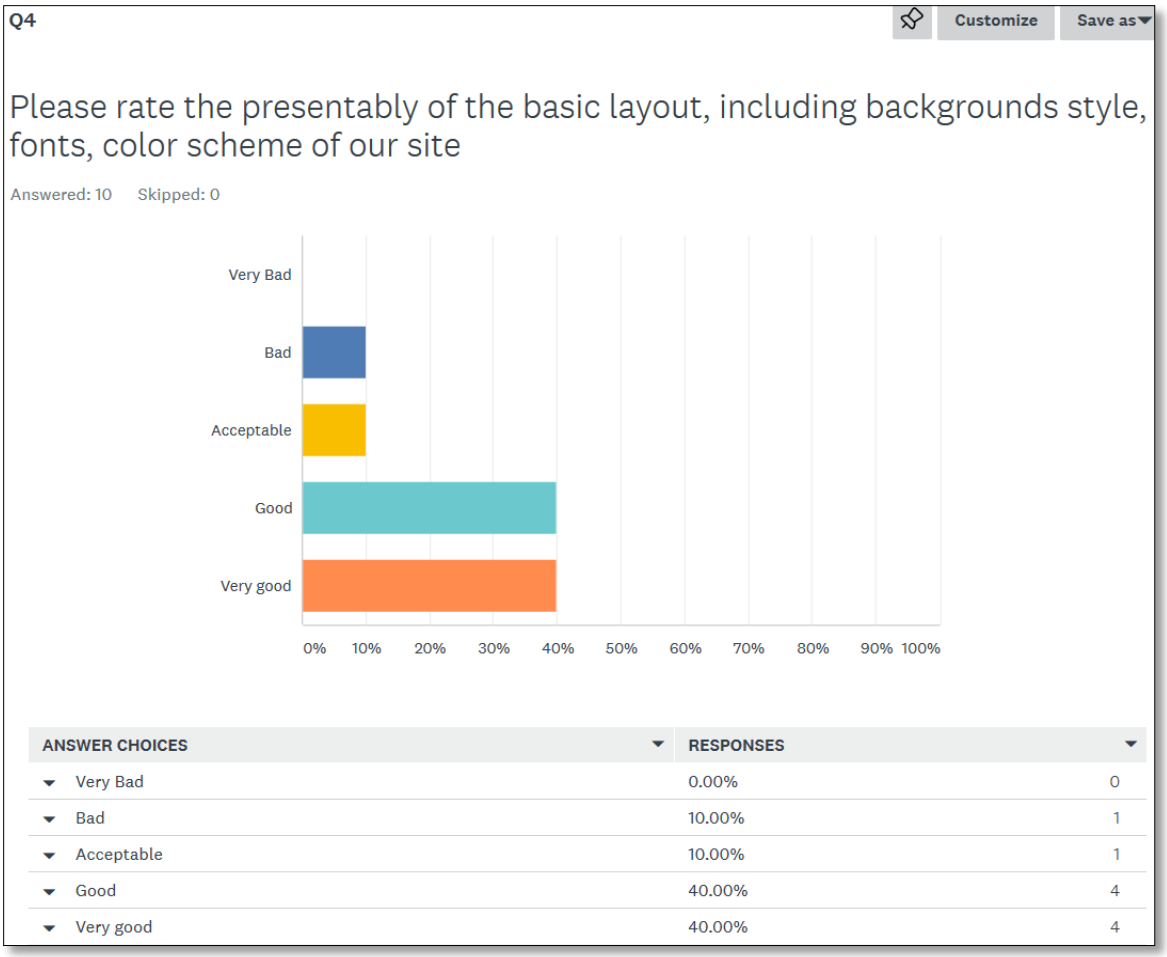
Q3

Please rate how navigable you found each individual page

	INTRODUCTION / HOME PAGE	RISKS WITH APP USE	APPS	APP SAFETY RATING SYSTEM	TERMS AND CONDITIONS	SNAPCHAT	INSTAGRAM	WHATSAPP	YOUTUBE	FAMILY-LINK	YOUTUBE KIDS	TOTAL
Not very navigable	33.33% 1	0.00% 0	0.00% 0	33.33% 1	0.00% 0	33.33% 1	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	3
Navigable but could be better	0.00% 0	0.00% 0	33.33% 1	0.00% 0	33.33% 1	0.00% 0	0.00% 0	0.00% 0	0.00% 0	33.33% 1	0.00% 0	3
Easily navigable	50.00% 5	0.00% 0	10.00% 1	20.00% 2	0.00% 0	0.00% 0	0.00% 0	0.00% 0	0.00% 0	10.00% 1	10.00% 1	10

Figure 300 Question 3 glitched and produced invalid results.

The intention behind question 3, was to allow for individual feedback on a per page basis allowing users to select as many pages as they wished to give feedback on. However, this question glitched and would only allow users to give selective feedback seemingly at random. While the original intent of the question was tainted by this, the data did serve a useful purpose. When viewed from the perspective of a sampling of pages the feedback can be viewed as positive, with some negative feedback resulting from users finding some pages too overloaded with content. This criticism we accept and were prepared for. Had we more time we would have broken the content down into more pages and allowed for more sections in content intensive sections. This would allow users to get a mental break more often as they consume the content. This is work we would endeavor to do in future work as we carry the service forward. These results serve to expand upon the findings of question 2.



ANSWER CHOICES	RESPONSES	
Very Bad	0.00%	0
Bad	10.00%	1
Acceptable	10.00%	1
Good	40.00%	4
Very good	40.00%	4

Figure 301 Here we see the results of question 4, aimed at gathering feedback on the overall presentability of the site.

Question 4 was designed to gather feedback on the overall presentability of the website including aspects such as readability, layout, style etc. The Feedback here was largely positive with 90% of survey participants rating the site from acceptable to very good. This was an area that concerned us as we elected to use an unusual style and bright colour scheme aimed at making the site readable for those with visual impairments and reading difficulties such as dyslexia. We were very happy to receive this largely positive justification of our choice.

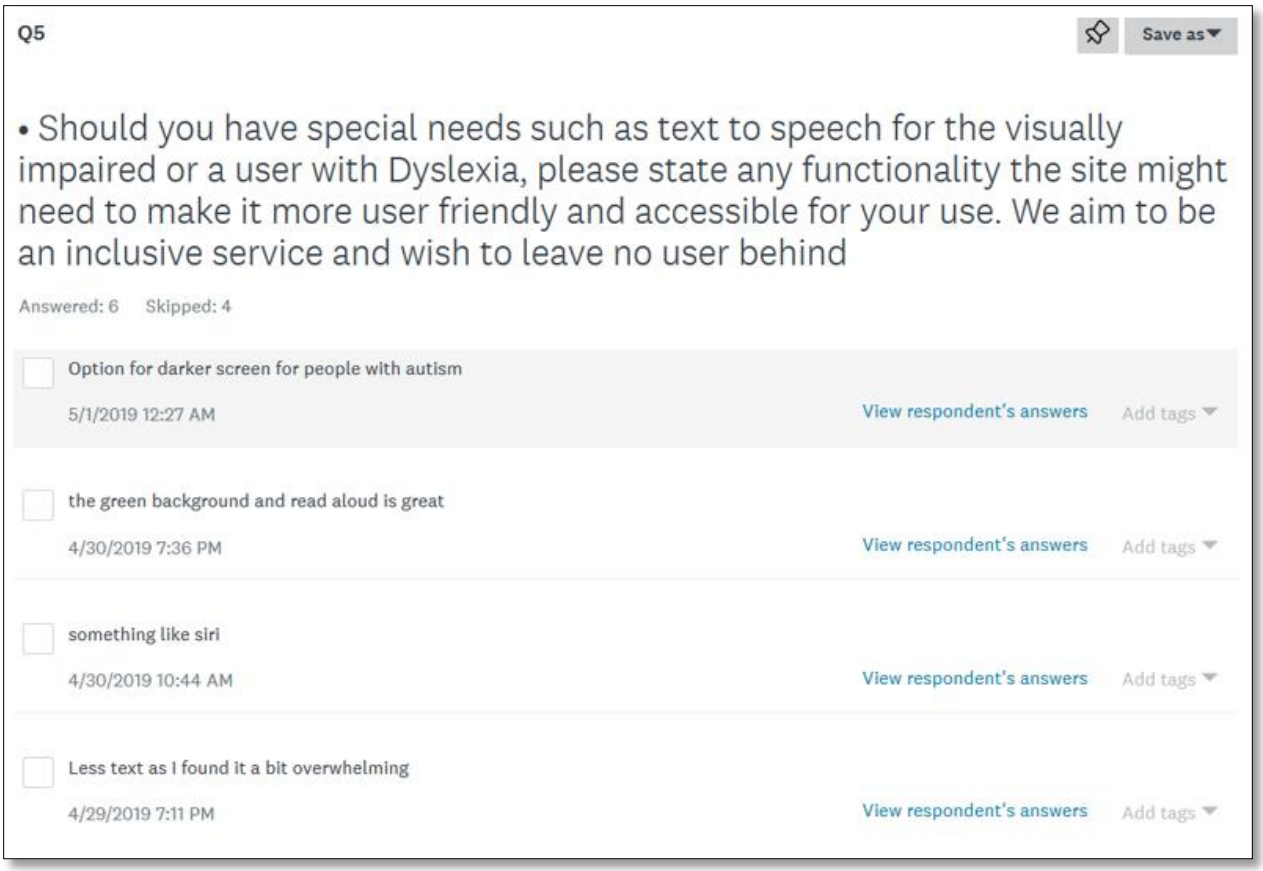
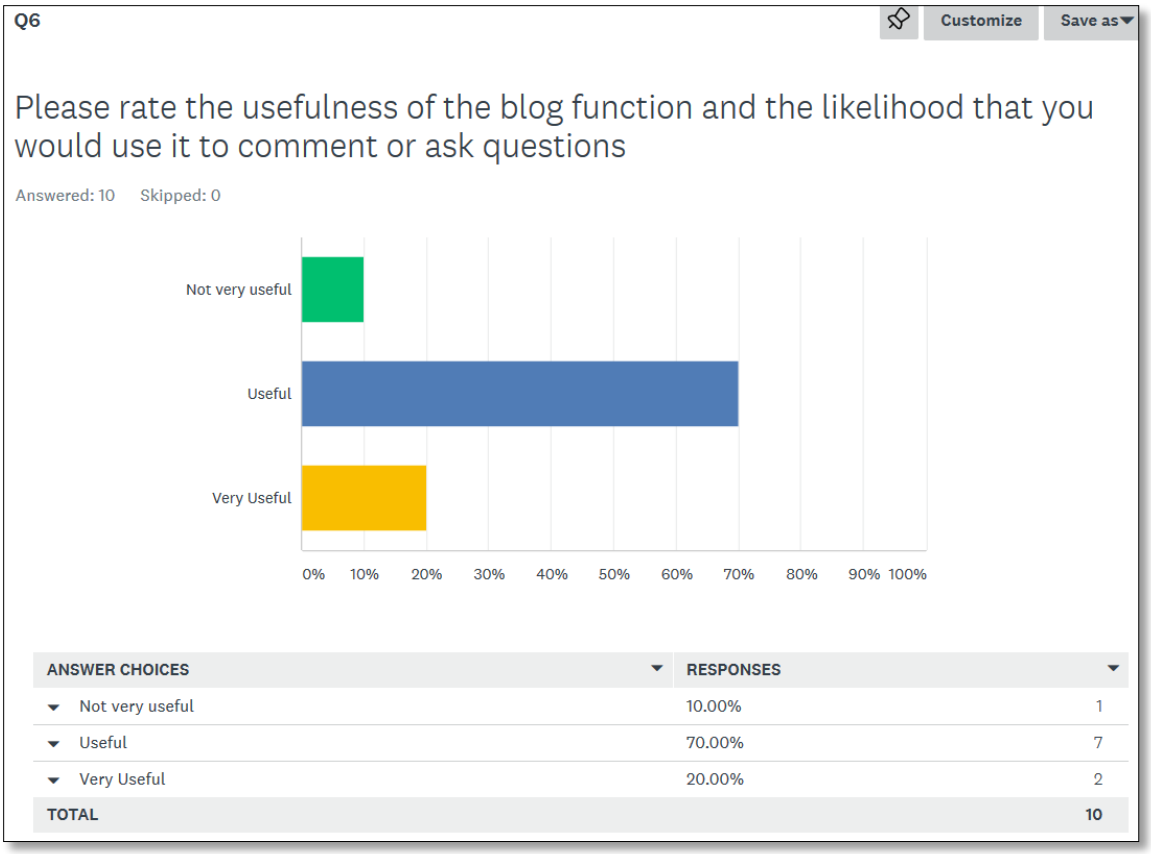


Figure 302 Here we see the interesting results we received from question 5

Question 5 was designed to illicit feedback regarding the usability of the site for those with impairments and provided an optional feedback for any services which user felt might add to inclusivity of our service. We had 4 very useful points of feedback here. One user Suggested a darker scheme or "dark mode" which would darken the screen for user with autism. This was a fantastic response which we greatly appreciated. We did indeed investigate the addition of this option but sadly the dark mode plug ins currently available for WordPress are still in beta. This is an addition would love to include should the plug in emerge from beta or we switch our website to a custom website design outside the WordPress development environment.

Another interesting feedback was from a user who revealed to us during testing that the user suffered from dyslexia. Our choice of colour scheme was proven to the right choice here as the tester informed us that the colour scheme, unlike other websites was very useable in this format despite the condition. This tells us that for inclusivity, future revision of the website was possible should include a light and dark mode.

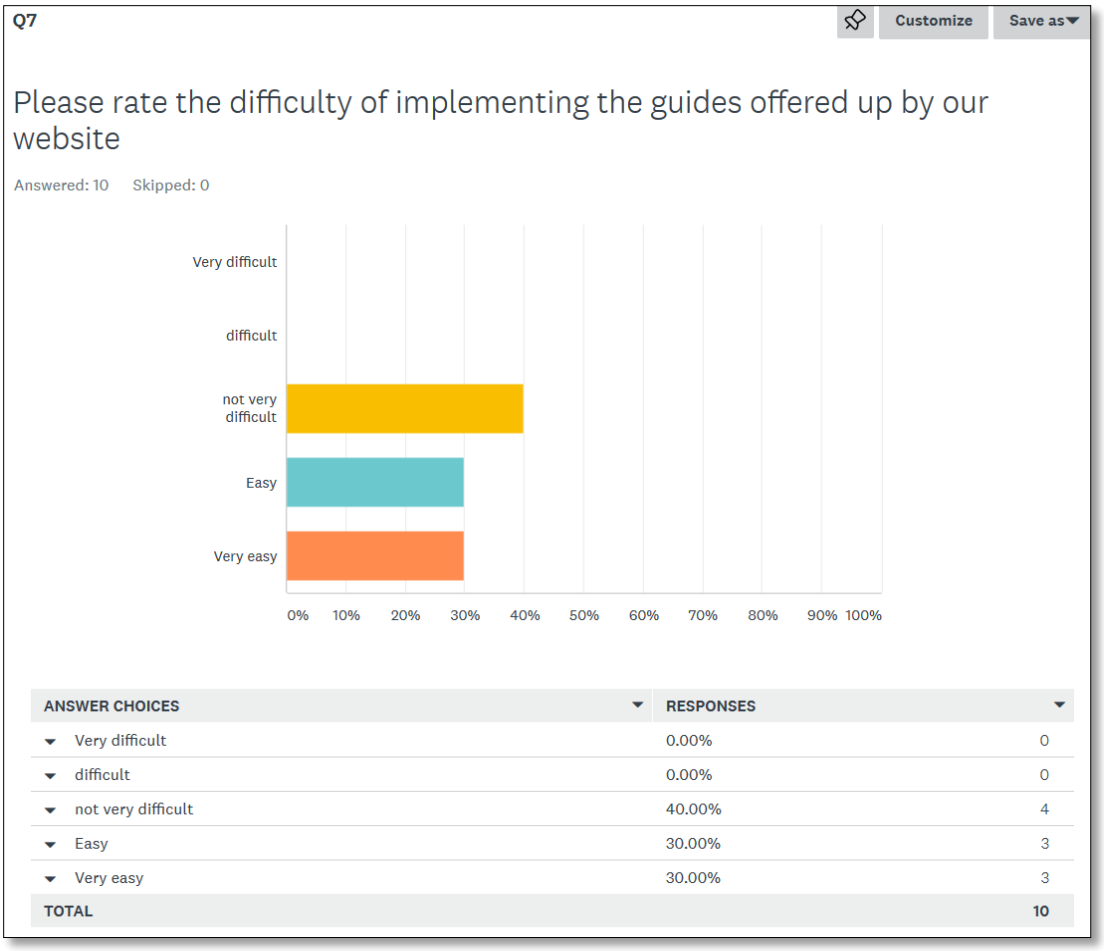
Finally, we got another reminder that some user did indeed find the amount of text over whelming. Future revisions of the site will include breaking the content into more sub sections and breaking up content with more breaks in sections.



ANSWER CHOICES	RESPONSES	
Not very useful	10.00%	1
Useful	70.00%	7
Very Useful	20.00%	2
TOTAL		10

Figure 303 This question was designed to gather feedback on the usefulness of our blog function. Most users found the feature useful.

Question 6 aimed to gather feedback regarding the usefulness of our provided blog function. While most users did find this feature useful, we have not had any users attempt to make posts that are not spam bots. We shall monitor this and perhaps encourage users to post question as the service matures and grows. However, we are encouraged to see that our spam filters are functioning properly.



ANSWER CHOICES	RESPONSES	
Very difficult	0.00%	0
difficult	0.00%	0
not very difficult	40.00%	4
Easy	30.00%	3
Very easy	30.00%	3
TOTAL		10

Figure 304 Question 7 highlights our feedback regarding level of difficulty in implementing our guides.

The feedback from question 7 was very important. This question was designed to discover how difficult users felt it would be to implement the recommendations of our guides. The feedback here was again almost overwhelmingly positive. 30% rated the guides as very easy to implement, with another 30% rating the guides as easy to implement and 40% rating them as not very difficult to implement. No negative feedback was received which was precisely what our group aimed for with our guides. This justification, that our service meets the needs of the gap in service identified by our research has indeed been satisfied where the Apps we have elected to cover so far are concerned.

Interestingly, we feel these statistics line up very favourably with those documented earlier in the CyberSafeIreland 2018 report regarding their information sessions providing safety tips and guides centred around online content as seen in table 7, section 8.1 **(CyberSafeIreland 2018 page 25)**.

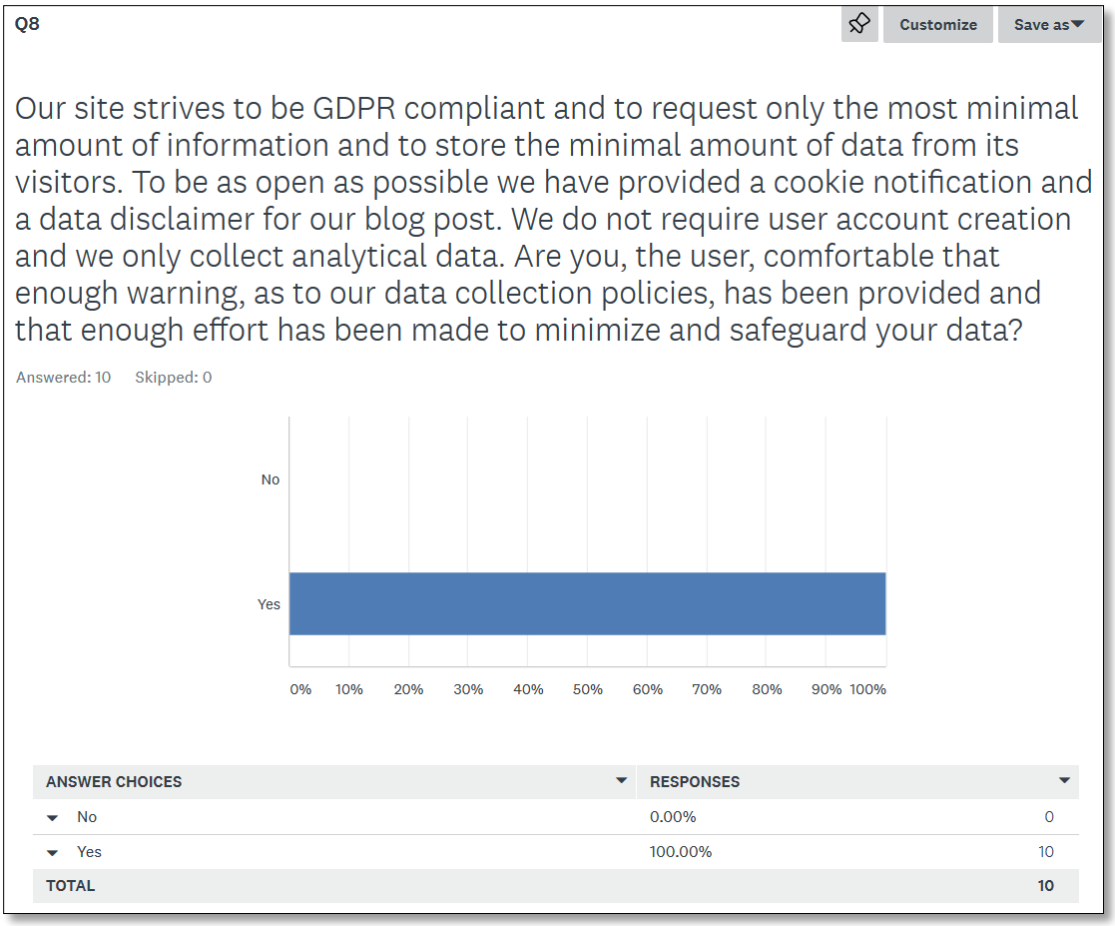


Figure 305 Question 8 is simply designed to determine if users feel they are anonymous enough while using our service.

Question 8 aimed to determine if visitors are happy with our GDPR implementation and disclaimers regarding data tracking, collection and sharing. Again, we see an overwhelming response here with 100% of survey participants happy with their anonymity while using the site and our warnings and disclaimers.

Question 9 was a general optional feedback question which only 3 users elected to answer and provided no useful feedback therefore we elected no to document this question.

Reflecting on the survey results and future work resulting from feedback

Our group found the survey results overwhelming positive and useful and we would like to express our thanks to our survey participants for their time and effort on our behalf. However, the results also highlighted some future work to be carried beyond the scope of our project. This work includes:

- Incorporating a switchable light and dark mode option as soon as a plugin becomes available our service is migrated to a custom designed service / website.

- We will need to add in extra section and break up content to make large sections of text more readable and allow users more mental breaks to mentally digest content as they proceed through pages. Furthermore, we will need to break up the app guides in sub-pages making the guides accessible.

- Each App section should become its own sub blog.

- We must design a marketing campaign to better reach our target demo graph. Due to time, financial and platform restrictions we feel that without a thorough marketing camping which can target specifically parents in Irelands we shall continue to struggle to gain traction with the target demo graph we would most like to reach. This was a known concern in so as far as we knew we might struggle to reach this demo graph within the time constraints of our project.

Overall, we feel the while there is room for improvement, the group feels that our site meets the deliverables as outlined in section 5.0 of this document. Our deliverables stated that we must produce a blog aimed at the Irish audience, we feel like the pertinent information that we set out to provide has been produced and successfully incorporated onto the site along with the scalability that comes with the website due to the analytics being set up allowing us to potentially set up a marketing campaign in the future to further bring a bigger audience to our website with regard to future work.

Google Analytics results from website launch period

Having plugged in the analytics for our website and being in the second week of the website being live it was time to review the data gathered to determine what lessons could be learned from it and what it could highlight for the future of the service.

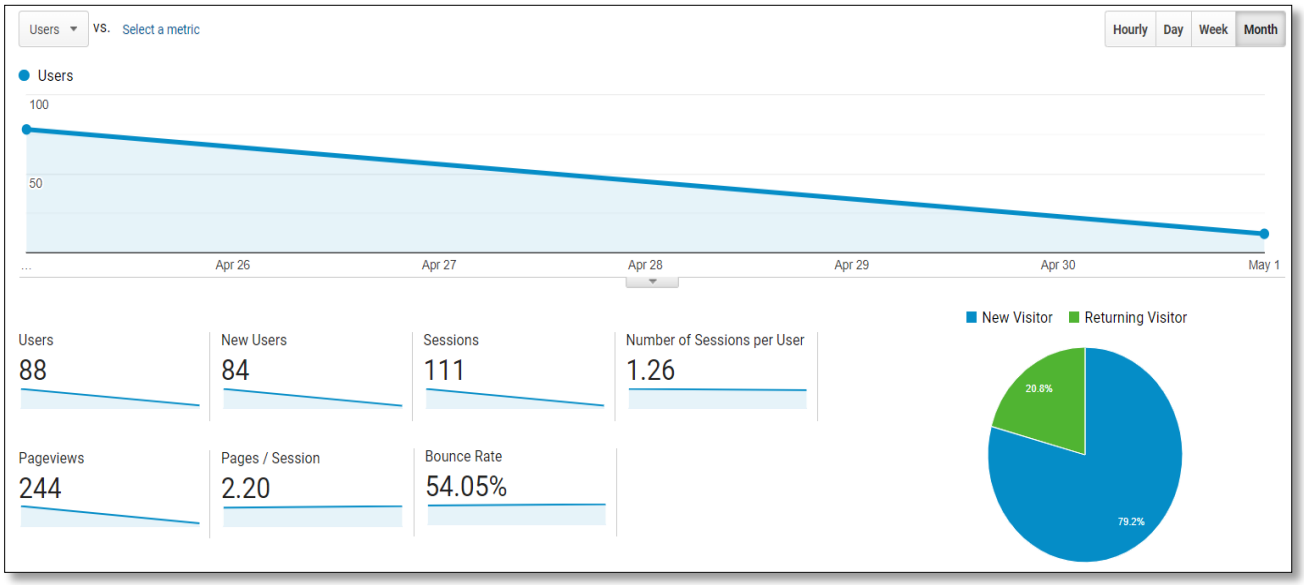


Figure 306 General overview of primary analytical data pertaining to www.safeappuse.ie website after two weeks live.

Firstly, we analysed the general activity data. Here we can see that almost 100 users have visited the site generating 111 sessions. This immediately suggests we have returning visitors. This is confirmed by the number of sessions per user averaging out at 1.26 and our new versus returning user ratio coming in at 79.2% versus 20.8%. This ratio tells us that roughly 20% of all visitors are returning to the website. We consider this a good start and it doubles the target that we originally aimed for in our initial reach which we set at 10%. With 88 users and 244-page views we can be sure that most users are not simply visiting one page but are actually engaging with the website. The one potentially negative figure that we see here is the bounce rate of 54.05% which mean that over half of our page views last under 1 second. However, we have not seen any attempted spam posts on the page, while a bounce rate of this number does suggest the website may be getting visited by spider bots this does suggest that our spam filter is working.

Page	Pageviews	Page Value
/	171	$0.00
/risks-associated-with-app-use/	38	$0.00
/about-us/	20	$0.00
/apps/	20	$0.00
/snapchat/	20	$0.00
/further-resources/	18	$0.00
/app-safety-rating-system/	10	$0.00
/our-research/	10	$0.00
/youtube/	10	$0.00
/whatsapp/	9	$0.00

Last 14 days PAGES REPORT

Figure 307 Pageviews per page on www.safeappuse.ie after two-week period

Secondly, we viewed the page views per page statistics of our website. We can see that surprising to no one the most popular page was the landing introduction page (here represented as /) with 171-page views in the last 14 days. Following the home page in popularity is the risks associated with app use with 38-page views showing that people are interested in the potential dangers apps may pose and are willing to learn. Followed by this is the about us page which is most likely people seeking out who made the service. Next is the main body of our website which is the apps page describing the content of our website in terms of apps and our methodology of how we researched each app. Followed by this is the snapchat blog page which contains the information gathered on how to secure it along with our best practice guides. This shows that the people who came to our website are interested in our content and specifically seem interested in securing snapchat.

One interesting statistic here is that, despite being leaps and bounds ahead of the rest in terms of quality of the guide compared to the others, YouTube didn't receive as much attention as we had originally thought. This means that we simply didn't achieve the reach we wanted to attract during the creation and publication of our website.

	Client Id	Sessions	
1.	1118088753.1556551633	4	(3.25%)
2.	1348139034.1556032414	3	(2.44%)
3.	1678810489.1556189703	3	(2.44%)
4.	1388054979.1556552882	2	(1.63%)
5.	1389954932.1556050567	2	(1.63%)
6.	1723235950.1556551995	2	(1.63%)
7.	1757752971.1556715144	2	(1.63%)
8.	1833719759.1556612447	2	(1.63%)
9.	1858429559.1556552113	2	(1.63%)
10.	2024982609.1556614854	2	(1.63%)
11.	2094952338.1556564177	2	(1.63%)
12.	2139920243.1556568170	2	(1.63%)
13.	2145003913.1556060566	2	(1.63%)
14.	400753946.1556550929	2	(1.63%)
15.	510756420.1556611755	2	(1.63%)
16.	521429009.1556556904	2	(1.63%)
17.	542622182.1556513154	2	(1.63%)
18.	544390177.1556044862	2	(1.63%)
19.	704169510.1556559262	2	(1.63%)
20.	815175790.1556658056	2	(1.63%)

Figure 308 here we see top 20 Client ID session data showing returning users

This data is encouraging as we can see from this data, we are getting a lot of recurring sessions meaning people are coming back to our website after they leave which is positive data.

	Operating System	Users	% Users
1.	Android	35	39.77%
2.	Windows	33	37.50%
3.	iOS	18	20.45%
4.	Linux	1	1.14%
5.	Macintosh	1	1.14%

view full report

Figure 309 Here we see users who come to our website based on operating system

Above we can see data relating to operating system usage of our users. Unsurprisingly we see a big showing for the Android platform at 39.77%. Desktop visitors also show highly at 37.50%. iOS also come in at 20.45%. There is a direct correlation here between our earlier data as derived from our own custom designed survey which showed that Android was both ahead and specifically ahead by 55% as seen in section 8.2 Table 11.

	Acquisition		
	Users	New Users	Sessions
	88	84	111
1 Direct	68		
2 Social	18		
3 Organic Search	2		
4 Referral	1		

Figure 310 Acquisition statistics for www.safeappuse.ie in two weeks

As we can see from our acquisition report for the website after two weeks, we see that most of our userbase is coming from direct links however we are seeing that slightly over 20% are coming over shared links over social media. While our current marketing strategy is having an effect, it is minimal, therefore if we were to take this project into further work, we must increase the reach and magnitude of our marketing strategy to reach our target demo graph. Some positive results from this report is that our search engine optimization is having some effect as 2 users did find our website via organic searches. While the results are very low, it does show that our website does show up for organic searches, so it is possible, from a marketing perspective, to spread awareness via our brand name.

Country	Acquisition	
	Users	New Users
	97 % of Total: 100.00% (97)	92 % of Total: 100.00% (92)
1. Ireland	**82** (84.54%)	77 (83.70%)
2. Canada	**4** (4.12%)	4 (4.35%)
3. United States	**4** (4.12%)	4 (4.35%)
4. United Kingdom	**2** (2.06%)	2 (2.17%)
5. Australia	**1** (1.03%)	1 (1.09%)
6. China	**1** (1.03%)	1 (1.09%)
7. Japan	**1** (1.03%)	1 (1.09%)
8. Portugal	**1** (1.03%)	1 (1.09%)
9. South Africa	**1** (1.03%)	1 (1.09%)

Figure 311 Here we can see the users who came to our website by location

Here we can see that most users who view our website are in Ireland which tells us that we have reached our demo graph in terms of market by country however, we are not reaching our specific demo graph inside the nationality of Ireland which would be parents or young children. This again suggests that we must have a better marketing strategy.

Overall, the data is initially positive. We see that we are getting positive results in terms of the ratio of page views to users. Also, we can derive that we are getting positive numbers of returning users to the site. This combined with the positive feedback of the site, this tells us there is potential for the future of the site if we take into consideration a better marketing strategy.

15.0 Glossary

API: Application Program Interface. A set or program routines, protocols or tools designed to make programming easier or access to data easier and faster.

Cookies: Cookies are pieces of data that are kept on the user's machine that can hold information that is needed on the website, usually something identifying the user.

Europol: Europol is the European Union's law enforcement agency. Their main goal is to achieve a safer Europe.

GDPR: The general data protection regulations which aim to set out legal guidelines regarding the privacy of both users and their data on-line, implemented on the 25th May 2018 designed by the European Parliament and the council of the European Union.

IGTV: Instagram Television, A channel provided within the platform, for users to post videos of either 10 minutes or 60 minutes maximum, within the Instagram platform

IOS: Apples mobile device proprietary operating system developed and maintained by the Apple corporation.

IP: Internet Protocol

Leetspeak: A common slang phrase meant to represent 'elite speak' which is where young people substitute letters with numbers with visually appear similar to the letters being substituted. For example, the word leet becomes l33t.

Meta-data: a set of data contain sub sets of data which combined allow for a large amount of information to be collected which paint a digital picture of a user and their online habits.

ooVoo: A video and text messaging client App.

Oireachtas: Legislative governing body of Ireland.

Phishing: attempting to extract information a user may not wish to reveal from users via email or digital message for malicious purposes.

PSNI: Police Service Northern Ireland

SEO: Search Engine Optimization

Sexting: This is the practice of sending explicit message containing sexually related content via a messaging or social media platform. While this is a practice often carried out between two consenting adults, it is obviously a grossly inappropriate practice to engage in with any child or indeed a non-consenting adult.

Snap: A picture taken through snapchat and sent to a friend or group.

SPAM: Irrelevant or unsolicited e-mail or digital message.

TLS: Transport Layer Security, the replacement for Transport Layer Security (TLS), one of the most widely used cryptographic protocols used to provide encryption for internet communications. Wherever you see HTTPS instead of HTTP, SSL has been deployed.

Talos: This is an intelligence network operated by Cisco telecommunications company, which consists of highly specialised security personal, hardware and software designed to track and monitor on-line activity particularly those kinds of activity pertaining to attacks and/or malicious internet usage.

UI/UX: User Interface (UI) and User Experience (UX)

Umlet: Umlet is a program used to document diagram such as use case diagrams or class diagrams in website, or program design documentation.

VPN: Virtual Private Network, which acts as a network proxy tunnel which is designed to obfuscate the users IP address.

Widget: an application plugin of an interface which performs a task or service.

16.0 References

_AdultCouple, (2019), Age inappropriate Instagram account. [ONLINE] Available from: https://www.instagram.com/_adultcouple/ [Accessed on the 20th March 2019].

Ahlgren M, (2019) Top 28 Instagram Statistics & facts for 2019. [ONLINE] Available from: https://www.websitehostingrating.com/instagram-statistics/ [Accessed 20th March 2019] Original Source: business.instagram.com.

An Garda Síochána (2018), Operation Ketch III. [ONLINE] Available from: https://www.garda.ie/en/about-us/our-departments/office-of-corporate-communications/press-releases/2018/october/operation-ketch-iii-2-10-18.html. [Accessed 20th March 2019]

Hotline.ie,(2017) Annual Report [ONLINE] Available from: https://hotline.ie/library/annual-reports/2018/hotline-annual-report-jan-dec-2017.pdf, pp. 16 [Accessed 20th March 2019]

SimilarWeb, (2019) Apple App Store Rankings[ONLINE] Available from: https://www.similarweb.com/apps/top/apple/store-rank/ie/all/top-free/iphone [Accessed 20th March 2019].

Bever L, (2019). A paediatrician exposes suicide tips for children hidden in videos on YouTube and YouTube Kids. [ONLINE] Published by the Washington Post Available from: https://www.washingtonpost.com/technology/2019/02/24/pediatrician-exposes-suicide-tips-children-hidden-videos-youtube-youtube-kids/?noredirect=on&utm_term=.c92ece095a94 [Accessed 26th February 2019].

Byrne S., Katz S.J., Lee T., Linz D., Mcilrath M, (2014), Peers, and Porn: Predicting Parental Underestimation of Children's Risky Online Experiences. [ONLINE] Oxford Academic, Journal of Computer-Mediated Communication Available from: https://academic.oup.com/jcmc/article/19/2/215/4067534, pp. 217 Paragraph 1 [Accessed 7th February 2019].

Cisco, (2019) Total Global Email & Spam Volume for February [ONLINE] Email & Spam Data, Total Global Volume Available from: https://www.talosintelligence.com/reputation_center/email_rep [Accessed 7th March 2019].

Claire M. (2018). Facebook and Snapchat being used to groom children as young as 7 in the Grimsby area. [ONLINE] Available from: https://www.grimsbytelegraph.co.uk/news/facebook-snapchat-being-used-groom-1464604. [Accessed 6th February 2019].

Computer Hope (2018), How do you know if an account is real of fake [ONLINE] Available from: https://www.computerhope.com/issues/ch001850.htm [Accessed on the 12th February 2019]

Curley C , (2019). The Momo challenge, what parents really need to know. [ONLINE]. Available from: https://www.theguardian.com/technology/2019/feb/28/viral-momo-challenge-is-a-malicious-hoax-say-charities [Accessed on the 7th March 2019].

CyberSafeIreland (2019), [ONLINE] Available from: https://cybersafeireland.org/ [Accessed on the 12th February 2019]

CyberSafeIreland (2018), Annual Report [ONLINE] Available from: https://static.rasset.ie/documents/news/2018/09/csi-annual-report-2017-final.pdf. [Accessed on the 12th February 2019]

CyberSafeIreland (2018), Annual Report produced 2017, released 2018. [ONLINE] Available from: https://cybersafeireland.org/media/1183/csi_annual_report_2017-final.pdf, pp. 17[Accessed 7th March 2019].

Czarina Lao (et al) (2017), Security Analysis on Snapchat. [ONLINE] Available from: https://courses.csail.mit.edu/6.857/2017/project/1.pdf [Accessed 7th March 2019].

Department of Justice & Equality (2019) Cybercrime [ONLINE], available from: http://www.justice.ie/en/JELR/Pages/Cybercrime, [Accessed 8th March 2019].

Department of Justice & Equality, (2018), Action Plan for Online Safety 2018-2019, [ONLINE]. Available from: http://www.justice.ie/en/JELR/Action_Plan_for_Online_Safety_2018-2019.pdf/Files/Action_Plan_for_Online_Safety_2018-2019.pdf. [Accessed 8th March 2019].

Department of Justice & Equality, (2018), Action Plan for Online Safety – Progress Report 2018-2019, [ONLINE]. Available from: http://www.justice.ie/en/JELR/Progress_Report_on_Action_Plan_for_Online_Safety_2018-2019.pdf/Files/Progress_Report_on_Action_Plan_for_Online_Safety_2018-2019.pdf [Accessed 8th March 2019].

Ducard M., (2019). YouTube Kids turns 2 and there's lots to celebrate!. [ONLINE]Published on the Official YouTube Blog. Available from: https://youtube.googleblog.com/2017/02/youtube-kids-turns-2-and-theres-lots-to.html [Accessed 26th Feb. 2017].

Gallagher C., (2018), Ten per cent of online child sex abuse images features infants. [ONLINE] Available from: https://www.irishtimes.com/news/crime-and-law/ten-per-cent-of-online-child-sex-abuse-images-feature-infants-1.3381322 [Accessed 7th March 2019].

GDPR (2019), The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. [ONLINE] Available from: https://eugdpr.org/ [Accessed 8th March 2019].

Gov.ie, (2019), BeSafeOnline, [ONLINE] Available from: https://www.gov.ie/en/campaigns/be-safe-online/ [Accessed 8th March 2019].

Goodbody W (2018) 18% of children talk to strangers online every day – report [ONLINE] Published by RTE.ie. Available from: https://www.rte.ie/news/ireland/2018/0910/992733-social-media-children/. [Accessed 8th March 2019]

Google (2019) Help your family create healthy digital habits. [ONLINE] Available from: https://families.google.com/familylink/ [Accessed 6th February 2019].

Google (2019) Privacy Check-up.[ONLINE] Available at: https://myaccount.google.com/u/1/privacycheckup/7?utm_source=google-account&utm_medium=web&continue=https%3A%2F%2Fmyaccount.google.com%2Fu%2F1%2F. [Accessed 24th February 2019].

Google, (2019), Safety Centre [ONLINE] Available from: https://safety.google/privacy/ads-and-data/. [Accessed 27th February 2019].

Gonzalez B. (2019). YouTube Movie Rental Service - Review. [ONLINE] Available from: https://www.lifewire.com/youtube-movie-rental-service-review-1846117. [Accessed 6th February 2019].

Guardian editors, et al, (2018) The Cambridge Analytica Files, [ONLINE]Available from: https://www.theguardian.com/news/series/cambridge-analytica-files. [Accessed 16th February 2019]

Heneghan C. (2016) Snapchat's popularity amongst Irish people is growing at a serious rate. [ONLINE] Available from: https://www.joe.ie/tech/snapchats-popularity-amongst-irish-people-is-growing-at-a-serious-rate-499013. [Accessed 6 February 2019].

Hotline.ie, [ONLINE] Available from: https://www.hotline.ie/ [Accessed 8th March 2019].

Hotline.ie, (2019), Filtering Software, [ONLINE] Available from: https://www.hotline.ie/internet-safety/filtering-software/ [Accessed 9th March 2019]

Hotline.ie, (2019), Internet Safety, [ONLINE] Available from: https://www.hotline.ie/internet-safety/ [Accessed 9th March 2019].

Hotline.ie, (2019) Make a Report, [ONLINE] Available from: https://www.hotline.ie/internet-safety/useful-websites/ [Accessed 9th March 2019].

Hotline.ie (2019) Safety Tips, [ONLINE] Available from: https://www.hotline.ie/internet-safety/safety-tips/ [Accessed 9th March 2019].

Instagram (2019), Community Guidelines. [ONLINE] Available from: https://help.instagram.com/477434105621119 [Accessed 9th March 2019].

Instagram (2019) Data Policy [ONLINE] Available from: https://help.instagram.com/519522125107875?helpref=page_content [Accessed 9th March 2019].

Instagram (2019) Terms of use [ONLINE] Available at: https://help.instagram.com/581066165581870?ref=dp [Accessed 9th March 2019].

Instagram (2019) Verified Badges [ONLINE] Available at: https://help.instagram.com/854227311295302 [Accessed 9th March 2019]

Webwise.ie (2019) Internet Safety [ONLINE] Available at: https://www.webwise.ie/saferinternetday/. [Accessed 8th March 2019].

Jenner K (2018) Instagram page, [Online] Available at: https://www.instagram.com/kyliejenner/ [Accessed 12th March 2019].

Julia, Google Employee & Member of the YouTube Help Community (2019), Our Response to the Momo Challenge & Character. [ONLINE] By Google. Available on https://support.google.com/youtube/thread/1917881?hl=en [Accessed on the 7th March 2019].

Krieger M. (2019), A Note on Security from Instagram's CTO [ONLINE] By Instagram.tumblr.com Available at: http://instagram.tumblr.com/post/164871973302/170901-news [Accessed 12th March 2019].

Lally C., (2018), Gardaí find 70,000 child sex images on man's computers [ONLINE] Published by the Irish Times, Available at: https://www.irishtimes.com/news/crime-and-law/gardaí-find-70-000-child-sex-images-on-man-s-computers-1.3381385. [Accessed 12th March 2019]

Lewis S. (2019), Kim Kardashian warns parents of "Momo challenge", but YouTube says it sees no evidence. [ONLINE] Published by CBS news, Available from: https://www.cbsnews.com/news/kim-kardashian-warns-parents-of-momo-challenge-youtube-take-action/ [accessed 7th March 2019].

Lou C., (2016) US Ad Spending 2015-2020 [ONLINE] Available From: https://bluemoondigital.co/wp-content/uploads/2016/12/eMarketer_US_Ad_Spending-eMarketers_Updated_Estimates_and_Forecast_for_2015–2020.pdf. pp. 19 [Accessed 12th March 2019]

Lucey A., (2017), Canadian who travelled to Ireland for sex with girl (14) sentenced. [ONLINE] Published by The Irish Times, Available from: https://www.irishtimes.com/news/crime-and-law/canadian-who-travelled-to-ireland-for-sex-with-girl-14-sentenced-1.3047329 [Accessed 7th March 2019].

Office of the General Prosecutor of The State of Tabasco (2019), High Risk Cyber police alert when playing challenges online. [ONLINE] Available from: https://www.fiscaliatabasco.gob.mx/Boletin/Index/16357 [Accessed 7th March 2019].

Omnicoreagency. (2019). YouTube by the Numbers: Stats, Demographics & Fun Facts. [ONLINE] Available from: https://www.omnicoreagency.com/youtube-statistics/. [Accessed 6th February 2019].

CyberSafeIreland, (2019) Parental Controls, [ONLINE] available at https://cybersafeireland.org/parents/parental-controls/ [Accessed 6th March 2019].

Patrick Kelleher (2019) Momo challenge: How the viral hoax took on a life of its own. [ONLINE]Published by The Irish Times. Available on: https://www.irishtimes.com/culture/tv-radio-web/momo-challenge-how-the-viral-hoax-took-on-a-life-of-its-own-1.3810964 [Accessed 7th March 2019].

PSNI (2019), PSNI Statement regarding Momo challenge. [ONLINE] Available from: https://www.psni.police.uk/news/Latest-News/250219-psni-statement-regarding-momo-challenge/ [accessed on the 7th March 2019].

Reilly J., (2019), Momo is dead. [ONLINE] The Sun, Available on: https://www.thesun.co.uk/news/8551299/momo-dead-suicide-challenge-game-statue-killed/ [Accessed 7th March 2019].

Rosen G., (2018) Security Update. [ONLINE] Available at: https://newsroom.fb.com/news/2018/09/security-update/. [Accessed 7th March 2019]

Ryan O. (2018) With 'Vulnerable' children contacting strangers, government launches 'internet safety resource' for schools'. [ONLINE] The Journal, Available from: https://www.thejournal.ie/children-contacting-strangers-online-3834649-Feb2018/ [Accessed 7th March 2019].

Safeappuse.ie, (2019) [ONLINE] Available from http://www.safeappuse.ie/ [Accessed 10th April 2019]

Sakuma, A. (2019), The bogus "Momo challenge" internet hoax, explained. [Online] Published by Vox. Available from: https://www.vox.com/2019/3/3/18248783/momo-challenge-hoax-explained (Accessed 6th March 2019].

Schechter E. (2016), Adding YouTube and Calendar to the HTTPS Transparency Report [ONLINE] Available at: https://security.googleblog.com/2016/08/adding-youtube-and-calendar-to-https.html [Accessed 12th March 2019].

SimilarWeb. (2019) Mobile App Ranking. [ONLINE] Available from: https://www.similarweb.com/apps/top/apple/store-rank/ie/social-networking/top-free/iphone [Accessed 7/3/2019].

SimilarWeb. (2019) Google Play Store rankings. [ONLINE]. Available from: https://www.similarweb.com/apps/top/google/store-rank/ie/all/top-free

Shneyder L.(2018) Creating Transparency with an Inbox Protection Rate. [ONLINE] Published by SendGrid. Available from: https://sendgrid.com/blog/inbox-protection-rate/ [Accessed 7th March 2019].

Snapchat. (2018) Community Guidelines, Snapchat [ONLINE] Available from: https://support.snapchat.com/en-US/a/guidelines. [Accessed 6th February 2019].

Snapchat. (2018) Privacy Policy [ONLINE] Available from: https://www.snap.com/en-US/privacy/privacy-policy/. [Accessed 6th February 2019].

Snapchat, (2015) What is Snapchat? [ONLINE] Available from: https://www.youtube.com/watch?v=ykGXIQAHLnA. [Accessed 6th February 2019].

Snapchat. (2018) Snap Group Limited Terms of Service. [ONLINE] Available from: https://www.snap.com/en-US/terms/#terms-row. [Accessed 6th February 2019].

Sweney M. (2013) More than 80% of children lie about their age to use sites like Facebook. [ONLINE] Available from: https://www.theguardian.com/media/2013/jul/26/children-lie-age-facebook-asa. [Accessed 6th February 2019].

Symantec.(2014) Embracing Android™ in the Enterprise [ONLINE] Available from: https://www.symantec.com/content/en/us/enterprise/white_papers/b-embracing-android-in-the-enterprise_WP_0514_21332808-en-us.pdf. pp. 2[Accessed 14th March 2019].

Staff Writer, (2018), New WhatsApp backup could put business char groups at risk of data breach, [ONLINE] Published by Business Tech News. Available from: https://businesstech.co.za/news/mobile/270923/new-whatsapp-backup-could-put-business-chat-groups-at-risk-of-data-breach/. [Accessed 6th February 2019]

Statistica.com, (2019), age distribution of worldwide Instagram users. [ONLINE] Available from: https://www.statista.com/statistics/248769/age-distribution-of-worldwide-instagram-users/ [Accessed 28th

February 2019] Original Source, Digital 2019: Global digital overview, page 108 [Online], available from:
https://datareportal.com/?utm_source=Statista&utm_medium=Data_Citation_Hyperlink&utm_campaign=Data_Partners&utm_content=Statista_Data_Citation.

Subedar A. and Yates W. (2017). The disturbing YouTube videos that are tricking children. [ONLINE] Available from: https://www.bbc.com/news/blogs-trending-39381889. [Accessed 8th March 2019].

Sulleyman A. (2018) WhatsApp Payments rolls out to some users, letting them transfer money to friends. [ONLINE] Published by Independent.co.uk. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-payments-money-transfers-users-accounts-friends-app-a8200546.html. [Accessed 6th February 2019]

Techerati (2017) Up to six million Instagram accounts affected by data breach. [ONLINE] available from: https://thestack.com/security/2017/09/04/up-to-six-million-instagram-accounts-affected-by-data-breach/ [Accessed 12th March 2019].

theouterlight. (2017). What is ElsaGate? [ONLINE] Available from: https://steemkr.com/elsagate/@theouterlight/what-is-elsagate. [Accessed 6th February 2019].

Trouvus (2019). How Does the YouTube Recommendation System Work? [ONLINE] Available at http://trouvus.com/how-does-the-youtube-recommendation-system-work/ [Accessed 7th March 2019].

unlimapps.com (2016) Snap + for Snapchat: UnlimApps Beta Repo. [ONLINE] Available at: https://beta.unlimapps.com/depiction/com.abcapps.snapplus [Accessed 6th February 2019] Source code repository available at: https://github.com/eni9889/SC-PP- [Accessed 6th February 2019].

Waterson J., (2019). Viral ‘Momo challenge’ is a malicious hoax, says charities. [ONLINE] Published by The Guardian, Available from: https://www.theguardian.com/technology/2019/feb/28/viral-momo-challenge-is-a-malicious-hoax-say-charities [Accessed 7th March 2019].

Watson M. (2019). YouTube is Facilitating the Sexual Exploitation of Children, and it’s Being Monetized [ONLINE] Available from: https://www.youtube.com/watch?v=O13G5A5w5P0 [Accessed 7th March 2019].

Wakabayashi’s D. (2018) Cybersecurity Firm Finds Way to Alter WhatsApp Messages [ONLINE]: Available from: https://www.nytimes.com/2018/08/07/technology/whatsapp-security-concern.html. [Accessed 12th February 2019].

Webwise (2018) BeInCtrl [ONLINE]. Available from: https://www.webwise.ie/beinctrl/ [Accessed 7th March 2019].

WhatsApp (2019), Data Sharing policy. [ONLINE]. Available from: https://www.whatsapp.com/legal/?eea=1#how-we-process-your-information [Accessed March 2019].

Webwise.ie, (2019), Explained: What is WhatsApp, [ONLINE] Available from: https://www.webwise.ie/parents/explainer-whatsapp/ [Accessed March 2019].

WhatsApp (2019), Privacy Policy [ONLINE]. Available from: https://www.whatsapp.com/legal/?eea=1#privacy-policy [Accessed March 2019].

Webwise.ie, (2019), Explained: What is YouTube? [ONLINE] Available from https://www.webwise.ie/parents/what-is-youtube/ [Accessed March 2019].

Webwise.ie, (2019), homepage [ONLINE] Available from: https://www.webwise.ie/ [Accessed 7th March 2019].

WhatsApp (2019), WhatsApp Terms of Service. [ONLINE]. Available from: https://www.whatsapp.com/legal?eea=0#terms-of-service [Accessed March 2019].

npc.ie (2019) Internet Safety Training Videos, Story. [ONLINE] Available from: http://www.npc.ie/online-training/internet-safety/story_html5.html [Accessed March 2019].

YouTube (2017) 5 ways we're toughening our approach to protect families on YouTube and YouTube Kids. [ONLINE]. Available at: https://youtube.googleblog.com/2017/11/5-ways-were-toughening-our-approach-to.html. [Accessed March 2019].

YouTube, (2019) Cable-free live TV is here. [ONLINE] Available from: https://tv.youtube.com/welcome/?ve=34273&utm_medium=ep&utm_source=youtube_web&utm_campaign=home [Accessed 6th February 2019].

YouTube (2019) Trending on YouTube. [ONLINE] Available from: https://support.google.com/youtube/answer/7239739?hl=en. [Accessed 6th February 2019].

YouTube Help Centre (2019) Disable or Enable Restricted Mode [ONLINE] Available from: https://support.google.com/youtube/answer/174084?hl=en&ref_topic=2803240 [Accessed March 2019].

Zuckerberg M. (2019) A Privacy-Focused Vision for Social Networking. [ONLINE] Available from: https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/ [Accessed March 2019].