ucc
Coláiste na hOllscoile Corcaigh, Éire
University College Cork, Ireland

**Final Year Project**

**Alison Buckley**

# ‘What are the key challenges faced by users of different age groups regarding online safety and data privacy and how can a digital platform address these challenges?’

**Supervisor: Krishnendu Guha**

**BA Digital Humanities and Information Technology**

**April 2024**

## Contents:



### 1. Abstract


As technology continues to integrate itself into our everyday lives, it is crucial to possess the necessary skills to ensure that we are well informed about online privacy and its complexities.

The objective of this project is to create a digital platform which educates people of all ages on topics related to online safety and data privacy. Three surveys were carried out on children, teenagers, and adults to identify knowledge gaps and to gather insights about what features and topics people would like to see on the platform. The platform has three main sections dedicated to the three groups mentioned above- each section is designed with the survey results in mind and offers age-appropriate content. The platform will feature a user-friendly interface and incorporates both visual and written elements.

The platform was built using HTML, CSS AND JAVASCRIPT. The platform offers various Interactive elements which allows users to engage with the content in several ways, catering to different learning styles.

An analytical section will also be present on the platform which showcases the survey results in a visual manner, graphs were created using python pandas. The educational platform ‘My Digital Compass’ aims to empower users to navigate the digital world safely by providing relevant resources and information on online safety and data privacy.

An interactive chatbot created using JavaScript will provide users with an alternative way to search for information on the platform.

## 2. Introduction

The digital has transformed the way we connect, learn, and interact with the world. While it offers undoubtable benefits it also presents a great number of challenges. Evidently, the complexities surrounding online safety and data privacy are ever evolving. With ‘53% of internet users concerned about protecting their privacy and 6 million experiencing cyber threats from 2015-2020’ (Lindner, 2023), it is clear that urgent action is needed to empower individuals to confidently navigate the digital world.

Evidently each age group face different challenges when it comes to technology and online safety, effective educational resources are needed to cater to the specific needs, learning styles and vulnerabilities of different age groups. Children may be unaware of basic online dangers; teenagers may struggle to navigate social media and adults might feel overwhelmed by constant advancements in technology. Understanding these unique challenges is essential when developing effective digital literacy initiatives.

To effectively answer the research question ‘What are the key challenges faced by users of different age groups regarding online safety and data privacy and how can a digital platform address these challenges?’ a mixed method approach is crucial. This strategy provides both qualitative insights into user experiences and opinions and quantitative data to identify broader trends across age groups, combining both ensures that the platform offers effective user-centric solutions.

This project adopts a human centric approach inspired by Industry 5.0, recognising that technology should serve and empower individuals by providing a personalised experience, ‘fostering stronger collaborations between humans and robots’ (Rushda, 2024). Industry 5.0 highlights how technology can be used to empower, support and augment human capabilities. This approach values the unique strengths of both humans with their creativity and judgement and machines with their precision and efficiency (Rushda, 2024).

The educational platform My Digital Compass will prioritise the individual needs and wants of each user offering a personalised and interactive experience for all. This will be achieved in several different ways; The surveys will guide the scope of the research revealing age-specific knowledge gaps and user preferences for features and content. This data driven approach will ensure that the platform offers features that directly address users concerns and learning preferences. By designing the platform with multiple demographics in mind it can encourage parents and children to learn about online safety together, this collaborative learning approach promotes open communication between generations.

An in-depth literature review will explore existing research to identify the broader societal challenges and knowledge gaps related to online safety and data privacy- highlighting the importance of digital literacy. An environmental scan will analyse existing educational platforms and related projects to learn from their success, identify potential gaps in current solutions and ensure My Digital Compass offers a unique and valuable contribution to the online safety space.

The implementation on an interactive chatbot on My Digital Compass will directly reflect the human-centric principles of Industry 5.0 offering a conversational way for users to get personalised answers to question they may have about online safety and data privacy. This puts human needs first, ensuring that users aren't left struggling to navigate complex information on their own.

My Digital Compass will incorporate a variety of engaging learning formats including videos, infographics, and interactive quizzes these elements will be created using JavaScript and a variety of different tools which will be discussed thoroughly throughout this report. This approach recognises that everyone learns differently and ensures a positive and effective educational experience for all users.

Ultimately the objective of this project is to create a platform for users of all ages to learn about online safety and data privacy, the environmental scan highlighted a significant gap, while numerous resources cater to parents and educators there are fewer options for adults seeking independent learning and children who want to explore online safety outside the classroom.

## 3. The Literature Review

**A literature Review examining online privacy concerns addressing challenges faced by contemporary society.**

**Introduction**

Digital Literacy is the 'ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies' (Unesco, 2018). As technology continues to integrate itself into our everyday lives, the significance of digital literacy is becoming extremely evident. Now, more than ever it is crucial to possess the necessary skills to ensure that we are well informed about online privacy and its complexities. Gilster suggests that Digital Literacy isn't just about knowing how to use technology, true digital literacy involves being able to analyse and understand the impact it has on society. (Bawden, 2008). Technology has made society's work easier, but this doesn't come without a cost, everyday our privacy is breached on both social media platforms and websites 'according to the 2020 Verizon Data Breach Report, 22% of breaches in 2019 were due to simple human error- things like an email being sent to the wrong person or an employee accidently revealing their login credentials' (Steele, 2021). Suggesting that data breaches, and information leaks commonly occur due to a lack of security measures taken by the user (Steele, 2021).

This literature review aims to explore Online Privacy closely examining ***Privacy and Surveillance***, ***The Introduction of GDPR, Covid-19 and the Digital Surge, and lastly discussing Age related challenges***, ultimately it aims to illuminate how digital literacy serves as an essential skill, providing us with the necessary capabilities to navigate the digital landscape effectively.

## Privacy and Surveillance.

'The legal definition of privacy refers to the right to be let alone: the right of a person to be free from unwarranted publicity' (Lyon, Zureik, 1996). However, it is evident that in terms of online privacy this isn't always the case. As technology is constantly evolving 'it is often difficult for users to determine how much of their data may be collected and how it might be used' (Acquisti et al., 2017), it is therefore becoming increasingly evident that gaining control over one's online privacy can prove challenging. There is a growing body of literature which suggests that our online privacy is constantly under threat as many companies and organisations forward user data to third party business partners, this data can contain personal information and could be used to 'identify a specific individuals; buying patterns, financial and health records etc' (Prince, Nessrine Omrani and Schiavone (2024).Data centric corporations are also storing, gathering and analysing user data at unprecedented levels, this increase is driven by intrusive technologies such as AI, GPS, data mining software, IoT based devices and many others (Prince, Nessrine Omrani and Schiavone (2024). Ioannou, Tusssyadiah and Miller(2020) point to the fact that these data breaches often occur without our knowledge, we may not even realise that our personal data is being sent to third party organisations let alone what data is being sent and what it is being used for.

Along with privacy comes surveillance which prior to technological advancements was limited to physical observation but has undergone significant change in recent years.
The 1980's witnessed the onset of many debates and discussions surrounding both 'privacy and surveillance' which was fuelled by the rapid development of information technologies and the widespread implementation of computer systems for surveillance (Lyon, Zureik, 1996). It can be argued that online privacy aims to guard your online activities and protect your personal information (Steele, 2021). However, surveillance on the other hand involves monitoring, collecting, and storing user data. As previously discussed, this can occur through the sharing of user information with third party companies who pay to place tracking cookies on pages belonging to other sites (West, 2019). Ioannou, Tusssyadiah and Miller (2020) (2020) highlights how in London a resident can expect to be captured on CCTV approximately 300 times each day. Furthermore, their car movements can be tracked via number plate recognition and their movements tracked using public transport (Oyster) cards. Additionally, their mobile devices can be used to monitor their movements on foot.
On the flipside Hagen and Lysne, 2016 argue that surveillance is extremely necessary as it can be used to detect criminal activity. 'Access to social media accounts and big data analytics could provide significant aid for law enforcement', CCTV footage can be used to identify suspects, predictive analysis can be used to detect possible terror attacks. CCTV surveillance cameras utilise algorithms for facial recognition and detection of suspicious behaviour (Johann Čas et al., 2017).
It is evident that many authors discuss the negatives associated with privacy and surveillance, however Waldo, Lin, and Cox (2010) suggest that we are quick to blame technology when it comes to privacy and surveillance related concerns, but society plays a significant role as well. They point out that 'Employers are demanding more information about employee… intensive work monitoring…members of the public demand information as well, individuals also demand information from each other in many contexts' (Waldo, Lin, Cox, 2010). As technology constantly compromises our right to privacy, it is apparent that our societal desire for access to people's information adds fuel to the fire.

## The introduction of GDPR

In recent years much research has focused on understanding public perception of data privacy intrusions, aiming to assist people in making informed decisions and ensuring people understand their rights before signing over their data. To govern these privacy concerns the European Union introduced The General Data Protection Regulation (GDPR) which came into effect in 2016. This policy establishes new regulations for data protection and privacy, The policy aims to empower consumers by giving them control over their personal data (Zaeem and Barber, 2020). As outlined by Zaeem and Barber, 'Its key principles include 'fairness and transparency, data minimisation, accuracy, storage limitation, integrity and confidentiality(security) and accountability'.
In an article published by P. Romansky and S. Noninska (2020) they state that the new European regulation GDPR changed the concept of privacy reassuring people of their 'right to be forgotten/to be erased', however P. Romansky and S. Noninska later argue that some websites and companies may not provide sufficient information about their privacy policy or require users to enter large amounts of personal information which isn't actually needed, this violates the GDPR principle of 'limited personal information, another issue they propose is the fact that companies may store multiple copies of users personal data meaning that your data could be located anywhere in the global network, this contradicts the GDPR policy-minimisation of data which aims to minimise stored and personal data. The points discussed in this article prove that even though GDPR promises users 'the right to be forgotten' this isn't always the case 'the user cannot be sure that all copies of personal data are 'erased'.

A study by Herrle and Hirsh (2019) revealed that after the introduction of GDPR, people were more likely to click 'I agree' and 'I accept' when presented with privacy notices on websites and applications. This could be due to increased trust in the new GDPR regulations, they felt that because the policy intended to standardise privacy and data protection laws across Europe and encouraged citizens to learn and understand their rights when it comes to their personal information (Herrle and Hirsh, 2019), users would therefore presume that all websites and companies were GDPR- complaint, making them feel comfortable agreeing to terms and conditions.

However, the study argues that when users are constantly presented with complex privacy policies when using a website, they are more likely to press accept as the act of quickly clicking a button allows them to access what they really came for. It is evident that companies must prioritise creating straightforward and easily understandable privacy policies. This brings us to the following consideration-

A consistent theme which was highlighted by several authors was the significance of heuristics which can heavily influence online privacy decisions.
'Heuristics are shortcuts in decision making that may lead to success but can also lead to errors' heuristics often come into play when individuals lack information and education on specific topics leading them to make decisions based on convenience rather than informed consent. In terms of data privacy this can cause several issues as when 'information, experience or time is limited people rely on heuristics' (Acquisti et al., 2017). This can be particularly detrimental in the digital age where decisions you make on websites and social media platforms can have lasting consequences in terms of your data privacy. It is therefore essential to acquire basic digital literacy skills to ensure that you are taking the necessary steps to protect your data. However, let's be honest, memorising every website's terms and

condition's is unrealistic, digital literacy doesn't imply having an exhaustive understanding of all the terms and conditions but rather knowing the necessary steps to take to safeguard your information.

## Covid-19 and the Digital Surge

'Internet technology is so pervasive today that it provides the backbone for modern living enabling ordinary people to shop, socialise and be entertained all through their own computers' (Arachchilage and Love, 2014).
The onset of the COVID-19 pandemic in 2020 forced a significant portion of society to transition both their personal and professional lives to a completely digital world as minimal social interaction was advised by governments worldwide, suddenly we were completely reliant on technology. Research highlights how 'the pandemic has exacerbated online privacy threats and the importance of addressing such threats to protect user welfare' (Yaraghi, Lai, 2022). As organisations have become increasingly 'virtual there has been a technological shift from work to the domestic environment' (Arachchilage and Love, 2014). This opens the door to several different challenges. Individuals working remotely may lack the necessary resources to protect themselves from cyber threats, their personal computers may not be as secure as the computers found in a centralised office environment (Arachchilage and Love, 2014).
The pandemic also prompted older generations to embrace communication technology to sustain connections during social distancing (Alagood, Prybutok, 2023). 'For many non-users of the internet, the pandemic became a catalyst for adoption and use' (Zapletal et al., 2023), 'forcing' the older generation to either adapt or be left behind, as those without digital skills during the pandemic were at a severe disadvantage.
However, for people who had not grown up surrounded by technology, this transition was extremely overwhelming, prior to the emergence of COVID-19 these individuals might have had limited knowledge on how to use online applications and may have lacked understanding on online privacy and its complexities, therefore it was a completely new environment for these individuals. Multiple authors have stated that the older generations were therefore more vulnerable to scams, data breaches and other similar threats without the necessary knowledge to be mindful and aware of these issues. A study carried out by Zapletal et at, 2023, found that during the pandemic older adults strengthened their digital literacy skills, enabling them to stay connected to friends, family, and their local communities. When clubs and groups moved to online platforms like Zoom, many older adults learned how to participate in video calls. This newfound digital skill helped combat loneliness and allowed people to continue participating in their activities (Zapletal et al., 2023).
While research on technology's role in healthcare during COVID-19 is established, the broader impact of the digital surge on individuals and society remains a relatively unexplored area. Further studies are necessary to fully comprehend the consequences of this rapid digital shift.

## The Digital Divide: Age related challenges.

Each specific age groups faces different challenges when it comes to online safety and data privacy, it is important to address these challenges for a more comprehensive understanding:

### Age related challenges (Children)

The booming popularity of social media platforms like TikTok and Snapchat coincides with an alarming trend: very young children are using the platforms even though these apps have a

minimum age requirement of 13. Research suggests that even older children can struggle to comprehend the complexities of data privacy (Livingstone, Stoilova and Nandagiri, 2019). How can we expect younger children to comprehend such a thing if older children are struggling? Much research would suggest that children's voices need to be incorporated and considered when creating frameworks and applications about said topics. As Livingstone et.al, suggest effective support systems play a crucial role in safeguarding children's privacy online, however they argue that 'restrictive parenting has a suppressive effect' on children, a plan needs to be put in place which allows children to independently explore the internet paired with parental supervision in order help them acquire effective digital literacy skills.

Literature suggests that supportive communication between parents and children about the internet and monitoring access to digital media has shown to 'offset the negative effects' (Ramsay, Terras, 2016), proving that instructive mediation fosters good digital literacy skills in children.
A study carried out by Stoilova, Livingstone and Nandagiri (2020) highlights that children struggle to grasp the data collected about them online, they are aware of their 'digital footprint' but struggle to comprehend how it is stored and how and why it could be used. What doesn't help is that Explanations about data collection on websites and apps is often unclear and unreadable failing to cater to younger users who need age-appropriate content.

## Age related challenges (Teenagers)

Much research suggests that teenagers are not fully aware of the complexities of online privacy and struggle to understand the 'implications of sharing personal information online' (Vespoli et al. (2024), indicating that many teenagers are unaware of the potential long-term consequences of their online data (Vespoli et al. (2024). Similarly Safe Search Kids highlight how most teenagers don't know that there digital footprint is traceable and could cause complications in the future if they have posted harmful or inappropriate content in the past.

Internet addiction among teens is becoming a real pressing issue, it involves becoming over dependant on the internet. (Sadhir, Stockburger and Omar, n.d.), this type of behaviour can regularly be observed when analysing teenagers use of the popular platform TikTok. According to new research 'many teenagers develop a pathological dependence on the platform' (Tarzana Treatment Centers, 2022). As TikTok features short videos powered by algorithms which show you exactly what you want to see it has the potential to foster addictive behaviours. More research is needed to determine the overall affects of addictive behaviour on social media platforms such as TikTok analysing the long-term implications.

Research including Steinfeld's 2021 study, demonstrates a clear correlation: limited parental involvement increases risk factors for teenagers online, leading to a higher likelihood of engaging in risky behaviour online. Active mediation among teenagers and parents aims to promote shared learning experiences and open communication between both parties. A digital platform tailored to both teenagers and parents could foster collaborative learning.

## Age related challenges (Adults)

Literature suggests that younger generations are influencing the older generations when it comes to acquiring digital literacy skills. ‘it’s the kids who influenced me…. They’re the ones who influenced me to get online’ (Zapletal et al., 2023). Similarly, Ivan and Fernández-Ardèvol (2017) state that children and grandchildren bridge the digital gap for many grandparents by helping them get online and setting up their devices. However older people without children or younger relatives face greater challenges acquiring digital skills and technical assistance. A recent study carried out by Pew Research Centre indicates that millennials have ‘led older generations in their adoptions and use of technology’, they see the gap in knowledge as a positive as it encourages intergenerational learning between the generations (Supramani, 2023).

A study by Zeissig et al., 2017 highlights variations in privacy concerns across age groups, they demonstrate how older adults primarily worry about misuse of financial data, while younger individuals focus on privacy risks associated with social networking sites (SNS). While both groups value online privacy the specific threats they perceive differ. This distinction highlights the needs for age-tailored information and education regarding data privacy and online safety.

Despite the prevalent focus on online safety for children and young adults, research on specific challenges faced by older adults often referred to as ‘digital immigrants’- those who weren’t raised with technology is often overlooked. This lack of understanding hinders the developments of tailored support and resources, leaving this demographic vulnerable to unique online threats. My Digital Compass aims to bridge this knowledge gap by addressing the distinct online safety needs of adults.

### Conclusion

To conclude this literature review highlights the exponential growth of technology as well as the subsequent challenges we face in a rapidly evolving digital world. The erosion of privacy in the digital age is undeniable with corporations and third-party entities collecting and utilising vast amounts of user data. While measures like GDPR offer some degree of protection, the literature highlights the crucial role of individual awareness (Digital Literacy). Users must carefully consider the implications of accepting terms and conditions before clicking ‘I agree’.

The digital surge during Covid-19 highlighted the importance of attaining digital literacy skills especially among older generations. Significant challenges persist particularly for older adults who lack exposure and technical expertise enjoyed by younger generations. Tailored educational content and initiatives are crucial to bridge the digital divide.

Children and teenagers also face unique challenges. It is evident that open communication and instructive mediation strategies are essential in helping children make informed choices about online activities and data privacy. Research indicates that teenagers often engage in

risky online behaviours, such as oversharing personal information on social media or interacting with strangers online. Teenagers may struggle to understand the long-term repercussions of their digital footprint. Parental guidance among teenagers can be limited therefore it is crucial that they are informed about online safety and data privacy so that they can make responsible decisions before doing anything online.

Digital Literacy is a necessity for all individuals in today's world. Ultimately, this review highlights the need for an educational platform catering to all age groups, preferences and learning styles. Further research should focus on the challenges faced by older adults ensuring that they too can become fully informed digital citizens.

There is a growing body of literature which suggests that supportive communication between parents and children about the internet and monitoring access to digital media has shown to offset the negative effects (Ramsay, Terras, 2016)

## 4. Environmental Scan

The purpose of this environmental scan is to assess the current landscape of publicly available web applications and educational platforms promoting online safety and data privacy. The literature review highlights various challenges users faces in an increasingly technology reliant world. Emphasising the urgent need for greater educational resources.

**What resources are currently available?**

It is important to understand what educational resources are currently available to the public regarding online safety and data privacy. By doing so we can understand how other people have approached the topic, see what is working and perhaps investigate areas in which more research and information is needed. Table 1.1(internal analysis) summarises key research findings, including website/project names, aims of the website, target audiences and areas where further research is needed. Table 1.2 summarises the websites capabilities e.g. website usability, tools etc.

Table 1.0

| **Name** | **Aims/Offerings.** | **Target Audience.** | **Gaps.** |
|---|---|---|---|
| **CyberSafeKids** | • Teach online safety.<br>• Provide kids with tools to stay safe.<br>• Talks/Resources for schools.<br>• Courses for parents/caregivers.<br>• Videos | • Kids<br>• Parents<br>• Teachers | • Major focus on adult mediation- no direct guidance for kids who want to learn independently.<br>• Limited engagement- |

| | | | |
|---|---|---|---|
| | • Interactive parenting guides. | | Due to the website's prioritisation of school talks, there is less assistance available directly on the web platform.<br>• Lack of resources for older adults. |
| **Webwise** | • Free information, advice, and resources to help parent, teachers and students address internet safety issues.<br>• Videos, webinars, youth events, campaigns,<br>• activities.<br>• Primary school and secondary school resources.<br>• Teachers' handbook.<br>• Parental advice | • Teachers<br>• Students<br>• Parents | • limited information for younger children- there are resources available, but they are harder to find as there is no section fully dedicated to younger children. (the search bar had to be used to find these resources).<br>• No resources available for older generations who don't have kids and want to learn about online safety. |
| **Barnardo's Online Safety Programme** | • Free parent webinars.<br>• Free e-books.<br>• Workshops for schools.<br>• Short videos for parents. | • Schools<br>• Parents | • No direct guidance for kids who want to learn independently.<br>• Limited tools.<br>• Not many interactive elements |

| | | | |
|---|---|---|---|
| | | | • Older adults without children should be considered too. |
| **internet matters** | • Guidance, advice, and support to keep children safe online.<br>• Inclusive digital safety.<br>• Advice guides.<br>• School resources.<br>• Videos.<br>• | • Parents<br>• Carers | • Website only targets parents who want to teach kids.<br>• More interactive elements aimed at kids.<br>• Information aimed at directly teaching children. |

Table 1.1

| **Name** | **Website usability** | **Tools** |
|---|---|---|
| **CyberSafeKids** | • Easy to navigate.<br>• Simplistic design- which makes it easy for parents to use. | • CyberSafeKids tool for schools- free online assessment designed to help schools evaluate their approach to online safety. |
| **Webwise** | • Clickable icons to each section (Teens, Parents, Teachers).<br>• Appealing layout.<br>• Each section contains relevant, age-appropriate information. | • Educational resources- downloadable PDFs.<br>• Videos for Primary and Secondary schools.<br>• Lesson plans for schools. |

| | | |
|---|---|---|
| | • Dropdown menus make the website easy to navigate. | |
| **Barnardo's Online Safety Programme** | • Basic structure.<br>• Simplistic design but effective.<br>• As the target audience is schools and parents it is clear and suitable for them.<br>• Slightly cluttered layout-some elements are hard to find. | • Workshops and talks.<br>• PDF fact sheets and guides.<br>• Reports on online safety trends.<br>• Collab/partnership with Google.org |
| **internet matters** | • Not visually appealing.<br>• Easy to navigate (the navigation menu is well structured.<br>• Inclusive (disabilities). | • Tool kits.<br>• Advice hub.<br>• Leaflets.<br>• Articles/Guides. |

**Key findings**

The environmental scan was carried out on five educational platforms, it revealed that there is a strong emphasis on supporting schools and parents within existing online safety platforms. While they deliver relevant information, there's room for improvement; more efforts could be made to ensure that kids can independently learn alongside parents. Incorporating more interactive elements would create an engaging user experience. A survey carried out for this research revealed that (get percentage for visual learning from my surveys) of people prefer to learn in a visual way. Including visual elements would allow people to retain more information. Noticeably the platforms offering workshops and talks seem to use their website to promote these services, they could broaden their impact by offering additional online resources. Most importantly there's a concerning lack of support for older adults who are becoming more technologically engaged. It's crucial to create age-specific resources addressing the online safety challenges unique to this demographic as they are often overlooked in current offerings.

An environmental scan of similar projects and papers was conducted to extract relevant insights before beginning the Digital platform 'My Digital Compass'. **E-safety and Web 2.0 for children aged 11–16 M. Sharples, * R. Graber, * C. Harrison* & K. Logan†.** This project analyses findings from surveys of children aged 11-16, teachers and parents. The findings from these surveys will help guide the creation of appropriate survey questions for this research project. Exploring the role that parents and teachers play in educating children

on safe social media usage can help determine if there are any gaps in knowledge while also examining how effective the current educational programs related to online safety are. Reviewing the results presented in this project will ultimately provide valuable insights.

The second project analysed was '**UK young adults: safety awareness online- is it a 'girl thing' by Sarah Pedersen.** This project interestingly explores is there are differences in online safety awareness between young men and women, investigating if girls and boys perceive online risks differently. Incorporating insights from this study will help determine how both boys and girls can be accommodated to ensure that they get the most out of an educational hub. To effectively address gender disparities, we must promote inclusive learning approaches that cater to all genders. Findings from this project would suggest that we need to develop online safety education platforms that are more effective and cater to specific needs and experiences of young men and women. By understanding gender differences, a more inclusive experience can be expected.

The third project analysed was **Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, Jiang, M., Tsai, H.S., Cotten, S.R., Rifon, N.J., LaRose, R. and Alhabash, S. (2016b).** The study examined how different generations perceive and understand online safety. They carried out surveys on 18 different focus groups. Noticeably older generations are becoming more involved with technology, so it is equally as important to include this age group when creating educational resources. The findings from this survey indicate 'online safety training is needed for all three generations but especially for older adults' (Jiang et al., 2016b). By surveying three distinct demographics, this project pinpointed generation-specific online safety concerns. This facilitates comparative analysis, revealing the unique needs of each age group and highlighting both shared experiences as well as clear gaps. Their findings on age-specific online risks will provide valuable context for this research project. While this paper offers valuable insights, it should be noted that since 2016 new platforms and online threats have emerged. It is also crucial to consult recent research to address this rapidly evolving landscape.

An article titled: ***Do digital natives value their online privacy? – Network Readiness Index*, Chauduneli, M. and Saxena, R. (2023).** This article highlights the challenge of balancing privacy and convenience for digital natives. While they value privacy, young users often prioritise ease of use, potentially leading them to accept privacy agreements without careful consideration. This suggests a need for simpler, more engaging ways to educate teens about data privacy. Additionally, this article prompts us to think about the potential benefits of collaboration between digital natives and digital immigrants to help bridge the gap and create a more informed online environment for everyone. This article directly supports the research question at hand as it addresses challenges faced by different demographics providing advice on how to better accommodate the specific needs of each age group. By examining perspectives of both digital natives and digital immigrant's new perspectives can be understood.

## 5. Tools and Methods

**Choosing the right approach.**

My Digital Compass is an educational platform catering to individuals of all ages from children just starting to explore the internet to adults navigating the ever-evolving digital world. It provides age-appropriate resources, interactive quizzes, a chatbot and various materials on online safety and data privacy.
A variety of tools and methodology were implemented to meet the needs of the research question.
A mixed method approach was carried out, this offers a more comprehensive understanding by leveraging the strengths of both qualitative and quantitative methods. Mixed method research allows for user input, as people's opinions and experiences are also accounted for, potentially eliminating bias which could be present in Quantitative research. Three surveys were carried using the mixed method approach on- adults (over 18), teens (13-17) and kids (9-12). The goal of the surveys was to assess current understanding of online safety, identify knowledge gaps and gather user feedback. This feedback included information on what features people would like to see on the educational platform as well as uncovering what learning styles the majority prefer. (visual or written materials and aids). Qualitative analysis was used to extract insights, patterns and meaning from textual and numerical data.

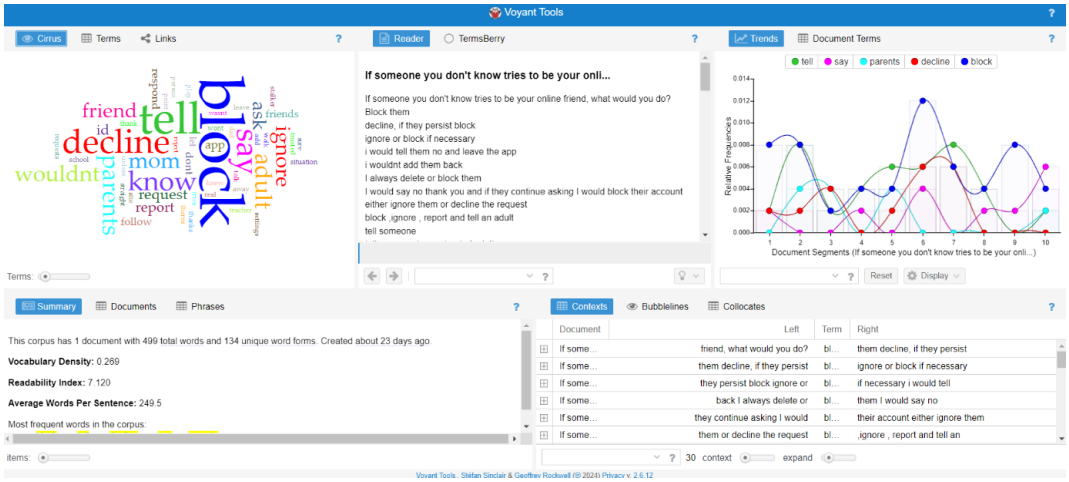
**Qualitative Analysis**

Textual analysis was carried out using Voyant. 'Voyant is a web-based text reading and analysis environment for digital text' (Voyant-tools.org). It is an open-source application providing 'text analysis such as word frequency lists, frequency distribution plots and KWIC (Key Word in Content) analysis' (ParadiseLostTutorial (n.d). Voyant offers a wider variety of tools, providing interactive and dynamic visualisations which help users gain insights into their text data. Voyant's visualisation tools were used to identify key themes in participants responses, particularly its word frequency Cirrus tool to highlight the most common words present in respondents answers. This allowed for connections to be made between age groups as well as notable differences.

**Voyant interface**

Figure 1.2 showcases the Voyant interface. The interface displays text analysis results from a survey of children aged 9-12. The survey question generated is 'If someone you don't know tries to be your online friend what would you do?'

Figure 1.2




**Cirrus:** The Cirrus tool is a word cloud which visualises the top frequency of words in a corpus or document. The terms that occur more frequently are larger and placed at the centre of the screen, as the size decreases so does the frequency with which they appear in the text. The colour of the words holds no significance.

**Reader:** The Reader tool showcases the content of the text in list form. You can scroll thought the content, hoovering over the words will show the word frequency again showing you how many times it is present in the corpus.

**Trends:** The Trends tool provides plots that represent the frequency of terms across your corpus, 'at the top of the graph a legend displays which words are associated with certain colours, you can click on the words in the legend to toggle their visibility' (ParadiseLostTutorial, n.d).

**Summary:** The Summary tool displays the number of documents in the corpus as well as displaying the total number of words present. It also showcases the top 5 most common words in the corpus which are indicated in the bottom left.

**Contexts:** 'The Contexts tool shows each occurrence of a keyword with its surrounding text (the context)' (ParadiseLostTutorial, n.d).

**Survey Development and Distribution**

Google Forms was the application chosen to create and generate the survey. Google forms was an optimal choice as it allows users to include different types of questions in your survey such as short answers, paragraphs, multiple selection, pull down questions, linear scale, and grids. Various question types allow for a diverse range of questions to be proposed. The data collected from Google forms is stored in the cloud which reduces the risk of losing data and results. Google forms is completely free to use and requires no technical expertise to get started making it an incredibly user-friendly survey creation tool. An advantage of Google forms is that once someone fills out your survey, the data can be accessed and viewed in multiple different formats. In the responses section you can see the results in a 'summary view, a question-based view and an individual responder view' (McPherson, 2019). Google forms automatically generates pie charts, bar charts and graphs offering immediate insights into your survey data. Once the form is created it is extremely easy to generate via email or

social media, it can even be embedded onto a website and can be accessed on any device. Using Digital surveys to gather results offers numerous benefits: respondents can complete the survey on any device as well as filling it out when they want, results are collected immediately eliminating printing costs and manual input errors. Google forms was ultimately chosen as the tool to carry out surveys for this research project, its intuitive interface allowed for the creation of surveys with various question types which enabled the collection of a wide range of data relevant to the research question.

Google Sheets, a free spreadsheet program included in 'Google's suite of tools' (Google, n.d.) offers another way to store and analyse the survey data collected though Google Forms. It is integrated into Google Forms meaning you can directly access a Google spreadsheet containing all responses. The spreadsheet updates as responses are added ensuring that you always have the latest data. Google Sheets is organised so that each response has its own row, with columns representing the questions and relevant answers. The organised structure of Google Sheets made it ideal for storing data from the three separate surveys. Since three surveys were completed, the direct transfer of findings from Google Forms to Google Sheets removed the needed for manual data entry which resulted in considerable time saving during the research process.

**Quantitative Analysis:**

'Since its first appearance in 1991, Python has become one of the most popular dynamic programming languages' (McKinney, 2013).

Python was used to analyse the survey results, specifically the python library Pandas which is used for 'working with data sets, it has functions for analysing, cleaning, exploring and manipulating text' (W3schools, n.d.). 'Pandas provides rich data structures and functions designed to make working with structured data fast, easy and expressive' (McKinney, 2013). It is an open-source data analysis and manipulation tool which allows users to create visually appealing graphs which are also easily interpreted by outside sources. Pandas was chosen for this project as it works seamlessly with CSV files and Excel spreadsheets, as the survey data was stored in a structured format, Pandas was a natural choice for data analysis and interpretation. Integrating Pandas with libraries like Matplotlib and Seaborn enabled the creation of informative and visually compelling charts and graphs. Matplotlib is the most 'popular Python library for producing plots and other 2D data visualisation' (McKinney, 2013). It is a foundational library necessary to create graphs. 'Seaborn builds on top of matplotlib and integrates closely with Panda's data structure' (seaborn.pydata.org, n.d.). Utilising Python Pandas enabled the survey results to be presented in a way that clearly highlighted trends, findings, and similarities deriving meaningful conclusions from the data.

Google Colab proved to be a well-suited environment for the analysis of the survey data. Google Colab is a hosted Jupyter Notebook service, enabling you to write and execute phyton code through your Google account. 'Colab notebooks are stored in a Google Drive account and include pre-installed Python libraries' (Burke, 2023), this offers an easy-to-use environment for generating immediate results. As the survey data was gathered using Google Forms and stored in Excel Spreadsheets importing the data to colab was efficient and hassle

free as it was loaded directly from the Google Drive. Colab offers outstanding performance, by running 'scripts in the cloud your local machine won't drop while executing your python scripts' (Reym, 2020). Colab is easily accessible from any web browser all that is required is an internet connection making it an ideal environment for data analysis.

Although Colab excels at data analysis using Python Pandas, its limitations mean it is not a web development environment as it is lacking built in support for core web development technologies such as HTML, CSS, and JavaScript. Colab notebooks isn't designed with web development in mind. However, if your website relies heavily on data colab can be used to analyse this data, it can then be implemented into your web application at a later stage.

**Web Development**

As colab was not robust enough to create a fully functioning website a different approach was taken to ensure that the requirements of the project were met, therefore Visual Studio Code was chosen as the coding environment. A hand coded web application was created using HTML, CSS, JavaScript, and PHP. HTML (Hyper Text Markup Language) is the standard markup language for creating web pages, HTML is used to define the structure of web pages. CSS stands for Cascading Style Sheets and is used to 'define styles for your web pages, including the design and layout of pages' (W3schools, 2019a). JavaScript is the 'programming language for the web, JavaScript can be used to update and change HTML and CSS, it can calculate, manipulate, and validate data (W3schools, 2019b). JavaScript can be used to make interactive engaging content. PHP (Hypertext Preprocessor) is a 'widely used open-source general purpose scripting language that is especially suited for web development and can be embedded into HTML' (PHP, 2019). PHP is an essential component when creating and processing forms, when a user submits a form, PHP code on the web server processes the input, allowing it to capture and respond to the user's data.

The website was hand-coded for several reasons. Firstly, it provided an opportunity to showcase the diverse web development skills acquired during my degree. Secondly, this approach offered maximum creative control over the websites design and functionality, ensuring seamless integration of interactive elements such as a chatbot and interactive quiz. the chatbot and knowledge quiz,

WordPress was also taken into consideration for this project however after weighing the options, the decision to make a hand-coded website was a more favourable choice.

**Why WordPress wasn't chosen.**

1. 'Only 1/3 of all WordPress installations are updated to the latest version' (Willsie, 2020. Websites that aren't updated regularly are vulnerable to security breaches which could potentially reveal users' sensitive data.
2. '94% of all infected CMS (Content Management Systems) are WordPress' (Willsie, 2020).
3. 'WordPress paints a bullseye on your website- it's really easy to determine if your website is built using WordPress… the majority of WordPress websites are hacked by

bots' (Willsie, 2020). Ultimately your WordPress site will be targeted by hackers simply because it is WordPress.

4. WordPress has limitations- 'while there are tens of thousands of plugins out there that can do pretty much anything, a developer would have to continue to add plugin on top of plugins to do things that could be done in a few lines of code' (Bravo, 2019). WordPress can be restrictive when creating highly customisable interactive elements.

'A hand coded website is fast, a lot faster than other types of websites... CMS like WordPress have a programming language behind the scenes such as python, php and so on, this is turn makes the website slower to load' (Slay Studios, 2023). Hand-coding a website minimises potential security breaches. Without plugins or databases there are fewer avenues for hackers to exploit.

As briefly mentioned above Visual Studio Code was selected as the development environment for this project. Visual Studio Code is a 'code editor redefined and optimized for building and debugging modern web and clous applications' (Microsoft, 2024), developed by Microsoft for Windows, Linux and macOS. It is designed to write, edit, and execute code. Visual Studio Code is packed with 'robust up-to-date features, offering a wide array of programming languages such as C++, Java and Python' (Tuama, 2022). Visual Studio Code offers a user-friendly interface which is extremely customisable, themes can be installed, and settings can be adjusted to suit user preferences.

FileZilla was used to transfer files from the local site to a remote site e.g. moving files to a web server so that it could be publicly accessible. FileZilla uses File Transfer Protocol (FTP) to securely transfer files 'between your local server and your FTP server' (arimetrics.com, 2023). SFTP is a more secure method and was used for this web application – SSH File Transfer Protocol is used to 'secure file transfers between a remote host server and a client user over a public network like the internet' (Thru Inc, n.d.). SFTP ensures continuous data protection as the connection is always encrypted whereas with FTPS the connection begins in an unencrypted state.

Leveraging survey results indicating a preference for visual learning, Canva a 'free-to-use online graphic design tool' (Canva, 2024) was used to create engaging infographics and posters for the platform. These visually appealing elements effectively communicated complex concepts and aligned with the learning styles of the target audiences.

To cater to different learning preferences particularly those who indicted a strong preference for video learning. Renderforest 'a cloud-based video creation platform (Gingerich, 2018) was used to create engaging explainer videos. These videos not only enhance the websites visual appeal but also effectively convey information in a format familiar to viewers who often consume content on platforms like YouTube (Survey results). This approach provides an alternative learning style to traditional text-based formats, potentially increasing user engagement and knowledge retention.

These will be explored in more depth in the Implementation and Analysis chapters.

## 6. Implementation

Utilising a combination of tools including Visual Studio Code for code development and FileZilla for file transfers, the platforms implementation commenced. HTML, CSS, and JavaScript formed the foundational structure. Additional tools were also used to enhance the platforms functionality and directly support the research aims of the project The platform aims to educate individuals of all ages about online safety and data privacy, providing tailored resources to address the unique challenges faced by different age groups. These challenges became evident throughout the literature review and environmental scan. For instance, confusion surrounding GDPR (General Data Protection Regulation), the digital divide between generations and the sudden digital surge during Covid-19 all underscore the critical need for individuals to continuously update their digital literacy skills. Studies highlight that older generations are embracing technology at a faster pace; children are becoming highly reliant on technology and teenagers can exhibit addictive behaviours. This combined creates a breeding ground for exploitation as scammers and companies target vulnerabilities in users' knowledge and behaviour which can ultimately put user data at risk.

Before creating the digital artefact, it was important to carry out surveys to establish knowledge gaps and understand what features and content people would like to see on the platform. This was implemented using Google Forms. Three surveys on kids, teenagers and adults were carried out to achieve a comprehensive understanding of online safety and data privacy across different age groups. To ensure accessibility each survey was created with age-appropriate language and content, an accompanying information sheet provided respondents with background knowledge about the aims and objectives of My Digital Compass. They were also informed of their anonymity throughout the survey as well as their right to withdraw from the study at any time.

Ethics approval was attained from The Social Research Ethics Committee (SREC) before conducting the surveys. This signed approval form can be found in the appendix.

The survey questions can be viewed in the appendix.

The kid's survey was distributed to local primary schools, the teenager survey was sent to local secondary schools and the adult survey was shared extensively on social media platforms as well as text and email. It was important to distribute the surveys to as many people as possible to gather a diverse range of answers for analysis. Higher responses help to facilitate a deeper understanding of the common concerns, challenges and specific needs required by each age group. The surveys were made available for two weeks. After the survey results were gathered and stored in the Google Sheet, the data analysis process could begin. Google Colab was chosen as the environment to do so. Each survey required its own analysis. Google sheets were converted to a CSV file (Comma-Separated Values).

As Google drive is linked to Colab it was extremely easy to upload each csv file as it could be directly mounted from the drive (see figure 1.3):

Figure 1.3

```
from google.colab import drive
drive.mount('/content/drive')
```

```
Drive already mounted at /content/drive; to attempt to forcibly remount, call drive.mount("/content/drive", force_remount=True).
```

```
import pandas as pd
df= pd.read_csv('/content/drive/MyDrive/dataset/Offical18fyp.csv')
```

Python Pandas was then employed to generate user-friendly graphs and pie charts. These visualisations aimed to clearly illustrate key trends, patterns and findings ensuring easy comprehension of the data.

See figures below:

Figure 1.4

df['How frequently do you review and update your online passwords?'].value_counts().plot.pie(ylabel="",title="How frequently do you update your passwords ",autopct="%1.1f%%",explode = [0.1, 0, 0, 0],legend=True).legend(loc=(1.1,0.7))

Reference- adult survey:

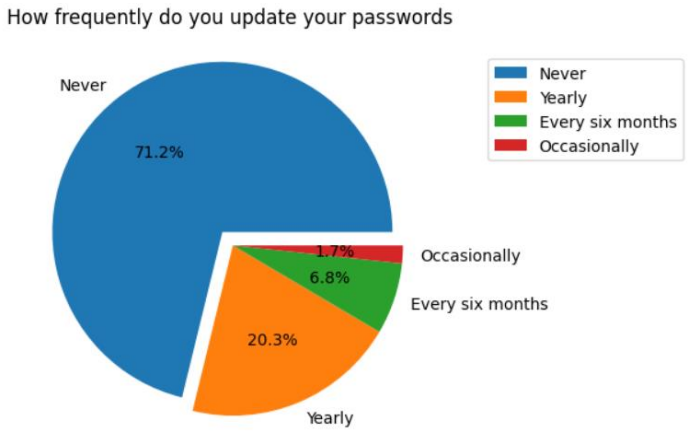



Figure 1.5

```
custom_palette = ["#2C3DEF", "#10FF00"]
df['Are you familiar with the the term GDPR? (General Data Protection Regulation)'].value_counts().plot.pie(ylabel="",title="Are you familiar with GDPR(General Data Protection Regulation?)
",autopct="%1.1f%%",explode = [0.1, 0],legend=True,
colors=custom_palette ).legend(loc=(1.1,0.7))
```

Reference- teen survey:

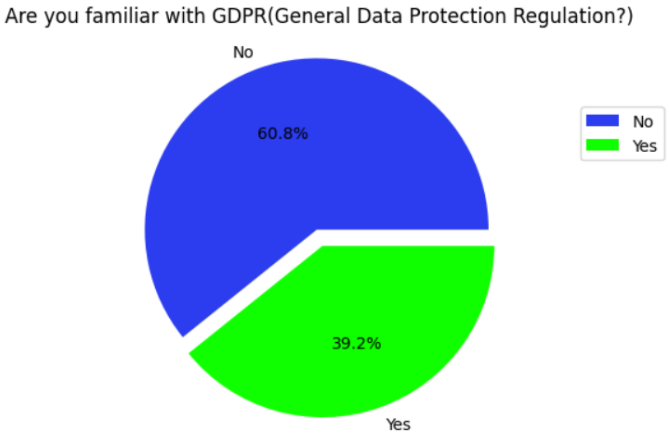
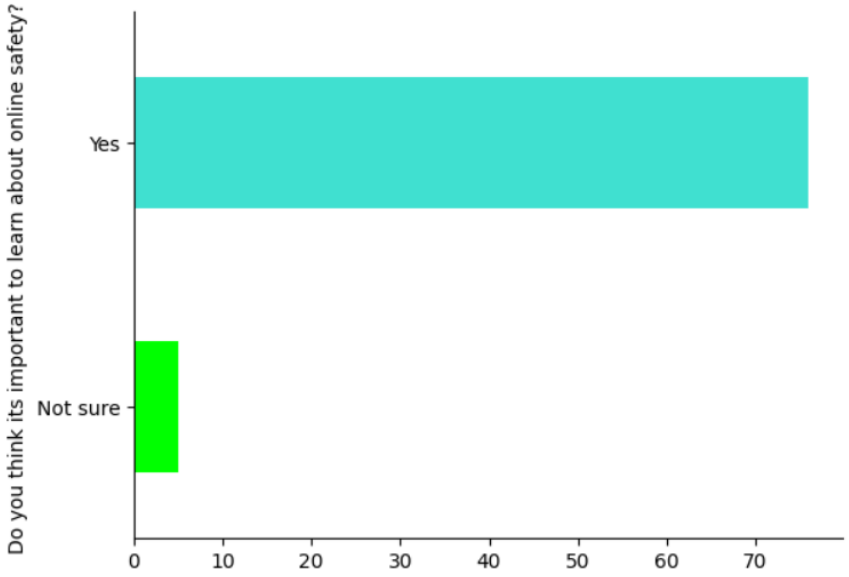



Figure 1.6

```
from matplotlib import pyplot as plt

custom_palette = [ "#00FF00", "#40E0D0"]
df.groupby('Do you think its important to learn about online safety?
').size().plot(kind='barh', color=custom_palette)
```

Reference- kids survey:




Vibrant colours were strategically chosen for the pie charts and graphs to make the survey results visually appealing. For the kids survey results brighter colours were favoured as they create a less intimidating atmosphere when interpreting the data. This approach aims to make the data engaging and accessible to all.

After the survey data was collected and insights were visualised, the next step was to design the platform utilising these findings to guide its development.

HTML provided the structural backbone of the platform, defining the content contained in all pages. CSS brought the website to life by styling elements in each of the pages. The homepage prioritised a simple yet impactful design. Strategic visual elements were included to immediately capture the user's attention and encourage further exploration. A blue background encompassed the home page of the platform, 'incorporating blue can evoke feelings of confidence, trust, and intelligence in users' (Fitzgerald, 2024). Promoting focus which is important for educational platforms. To accommodate diverse learning preferences, the homepage features both a navigation bar and visually engaging icons, offering multiple ways for users to explore content (see figure 1.7).

Figure 1.7


The name my Digital Compass reflects the platforms core purposes: empowering users to navigate the digital world. Just as a compass guides people in the right direction, the platform equips users with knowledge and resources to make informed decisions online.

Bootstrap was employed to create the navigation bar, ensuring seamless integration and optimal user experience (UI). As a responsive front-end framework Bootstrap ensures that different layouts can be adapted to different screen sizes, providing a consistent experience for users on all devices.

**Search Bar**

The websites focus was interactivity, UI was prioritised throughout to create an enjoyable experience for the user. A search bar was introduced on the Home page (see figure 1.8), this was powered by JavaScript and enables users to quickly locate relevant information allowing users to bypass the websites navigation bar and icons and find the information they need

instantly. The search bar was built using core JavaScript functions for event handling (form submission) and displaying of results. When a user inputs a search, it is compared to queries that exist within the JavaScript file, if the query matches it is then displayed in the form of a link to the user. Programming languages are extremely case sensitive for example the words gdpr and GDPR are considered different strings. Therefore, in the implementation of this search bar it was important to combat this issue. That is why. toLowerCase() was used, this method takes a user's query and returns a new string where all the letters have been converted to lowercase, the lowercase version is then matched against the page titles and links (the search results) in the JavaScript file. This method ensures that users will still find what they are looking for regardless of how they type it. This promotes a user-friendly search experience where results are reliably found regardless of input variations.

Example:

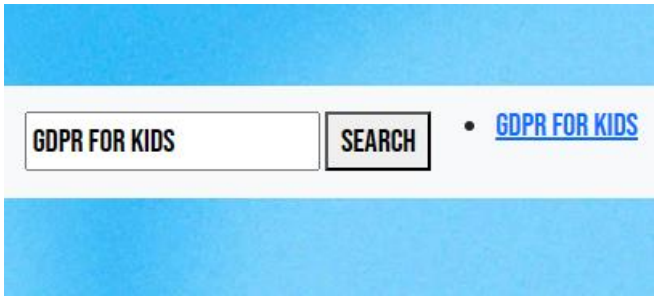
var searchQuery= "GDPR for Kids";

var lowercaseQuery= searchQuery.toLowerCase(); //this will now be "gdpr for kids"

the search will then be performed using lowercaseQuery.

Figure 1.8

Demonstration of the search bar:




**Knowledge Quiz**

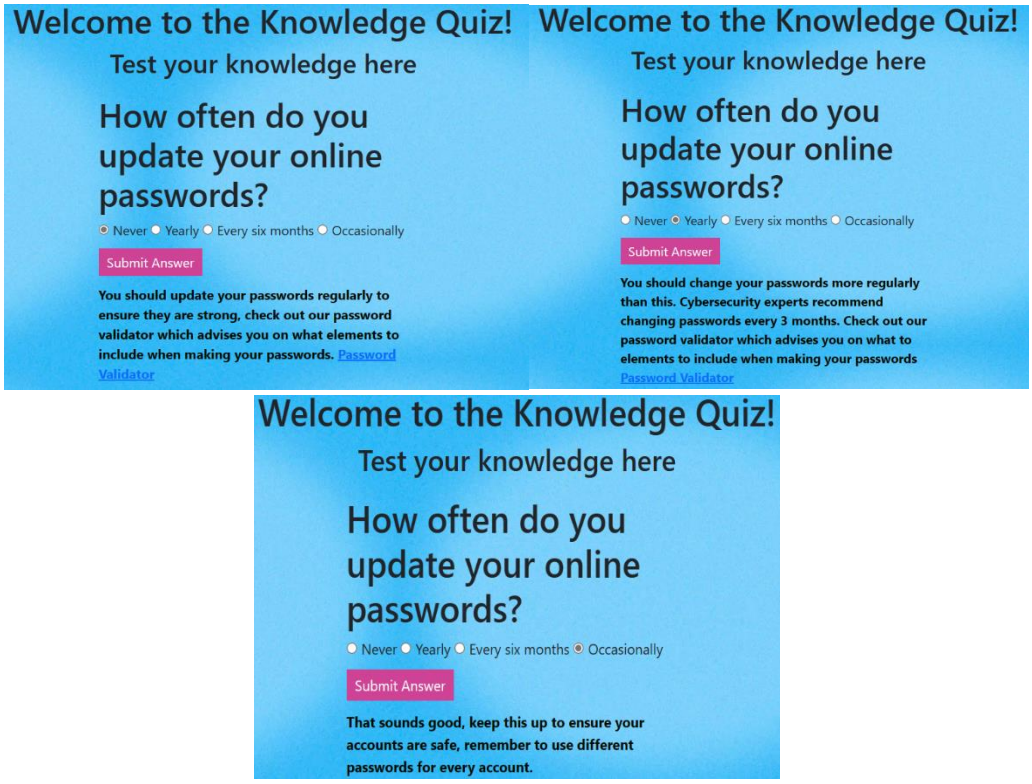
To personalise learning, knowledge quizzes were created using JavaScript, the three quizzes were created with an understanding of the online safety needs of every age group, tailoring each quiz to specifically suit user needs. The idea behind the quiz is that users are presented with questions about online habits etc, and can select which answer applies to them, they will then receive tailored feedback in the form of text as well as links to relevant information for a deeper understanding.

Figure 1.9

Select the quiz which applies to your age group:


Figure 2.0

Demonstration of quiz:




The JavaScript reacts to user input, gets the selected answer, creates the appropriate feedback message, and adds links where necessary (see figure 2.1 for the code related to the quiz).

Figure 2.1

```
document.querySelectorAll('.submit').forEach(function(button) {
  button.addEventListener('click', function() {
```

Code to be executed when the submit button is clicked.

```
switch (userAnswer) {
      case 'never':
        resultText = 'You should update your passwords regularly to ensure
they are strong, check out our password validator which advises you on what
elements to include when making your passwords. ';
        password1Link1 = "<a href='" + password1Link1 + "'>Password
Validator</a>";
```

```
        break;
```

The switch statement evaluates the userAnswer. ResultText adds the feedback as well as adding necessary links.

```
let finalResult = resultText;
    if (password1Link1 !== 'password.html') {
      finalResult += password1Link1;
    }
```

The finalResult variable is used to assemble to complete feedback for the user. It adds the text from resultText, additional links such as password1Link1 are then added if the code determines that they are relevant to the answer.

**Password Validator**

A password validator was implemented to promote the creation of strong passwords. The validator provides real time feedback on password strength by indicating (with ✓ or ✗) whether a user's desired password included elements like uppercase letters, lowercase letters, numbers, special characters etc. This feature provides people with advice on how to make strong passwords as well as a space to experiment and test potential passwords. The password validator was inspired by Sharathchandark's- 'Password Validation Check in HTML CSS & JavaScript'.

The password validator was implemented using JavaScript and HTML (see figure 2.2 for the code related to the chatbot).

Figure 2.2

```
<div class="password-check">
        <div class="check-length">
            <img
src="https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg"
/> At least 8 characters Long
        </div>
        <div class="check-uppercase">
            <img
src="https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg"
/> At least 1 uppercase letter (A-Z)
        </div>
        <div class="check-lowercase">
            <img
src="https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg"
/> At least 1 lowercase letter (a-z)
        </div>
        <div class="check-number">
```

```
            <img
src="https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg"
/> At least 1 number (0-9)
        </div>
        <div class="check-special">
            <img
src="https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg"
/> At least 1 special character (@-$)
        </div>
```

Above is the list of criteria which is displayed to the user along with a checkmark or cross to indicate whether the current password contains each element or not.

```
const combinations = [
  { regex: /.{8}/, key: 0 },
  { regex: /[A-Z]/, key: 1 },
  { regex: /[a-z]/, key: 2 },
  { regex: /[0-9]/, key: 3 },
  { regex: /[^A-Za-z0-9]/, key: 4 },
];
```

The combinations array defines the core validation rules that the password checker enforces.

```
<img id="ShowHide" src="https://cdn-icons-
png.freepik.com/512/6405/6405909.png" />
```

This creates the button with an eye icon allowing you to see or hide the password you have typed.

```
ShowHide.addEventListener("click", function (e) {
  validatorText.type = validatorText.type === "text" ? "password" : "text";
  e.target.setAttribute(
    "src",
    e.target.src.includes("https://cdn-icons-
png.freepik.com/512/6405/6405909.png") ?
"https://static.thenounproject.com/png/5584119-200.png" : "https://cdn-icons-
png.freepik.com/512/6405/6405909.png"
  );
});
```

This JavaScript runs when you click the eye icon, it toggles between hiding and showing the password as well as changing the image so that the icon is covered when the password is covered and opened when the password is visible.

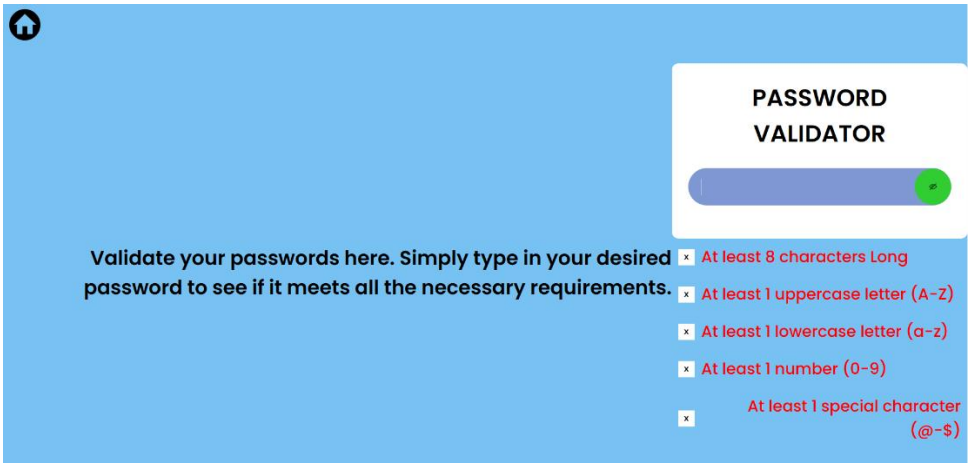
```
    if (IsValid) {
      checkItem.src =
"https://media.istockphoto.com/id/1079725292/vector/green-tick-checkmark-
vector-icon-for-checkbox-marker-
symbol.jpg?s=612x612&w=0&k=20&c=OvOpxX8ZFuc5NufZTJDbpwGKvgFUmfZjY68MICmEzX4=";
      checkItem.parentElement.style.color = "green";
    } else {
```

```
      checkItem.src =
"https://i.pinimg.com/736x/ec/81/36/ec813631b8f3541b2f3828936bca8286.jpg";
      checkItem.parentElement.style.color = "red";
    }
  });
});
```

This determines whether a specific password validation rule has been met. If the rule has been met the text colour of the rule description will turn green, the X image will turn to a green checkmark. If it has not been met the text will remain red and the X image will not change, this notifies the user that additional changes need to be made to ensure that the password is strong and meets all requirements.

The password validator features a simple, clean design with a blue colour scheme for an easy-to-use and visually consistent experience (see figure 2.3).

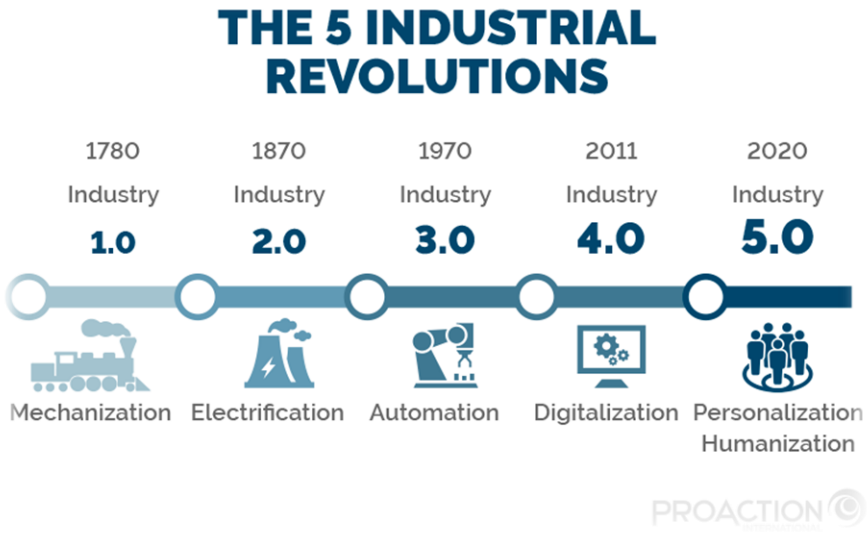
Figure 2.3




**Chatbot**

The inclusion of a chatbot on My Digital Compass offered an accessible way for users to find information. As research was conducted on how the platform could become more interactive and user focused. Industry 5.0 was discovered. 'Industry 5.0 is focused on humans and AI working together as well as bringing personalisation back into the market' (O'Callaghan, Gorato, McHugh, n.d.). Ultimately the revolution of Industry 5.0 will be more about giving a 'customised and personalised experience for consumers' (O'Callaghan, Gorato, McHugh, n.d.), providing convenient alternatives for human workers. 'The overall current state of understanding of Industry 5.0 describes it as a movement to bring the human touch back to the manufacturing industry, driven by the consumers desire for mass personalisation' (Akundi et al., 2022). User experience is at the heart of industry 5.0- 'the key to industry 5.0 success isn't the tech- it's the people using the tech' (Paula, 2022), (see figures 2.4 & 2.5 for visual descriptions).

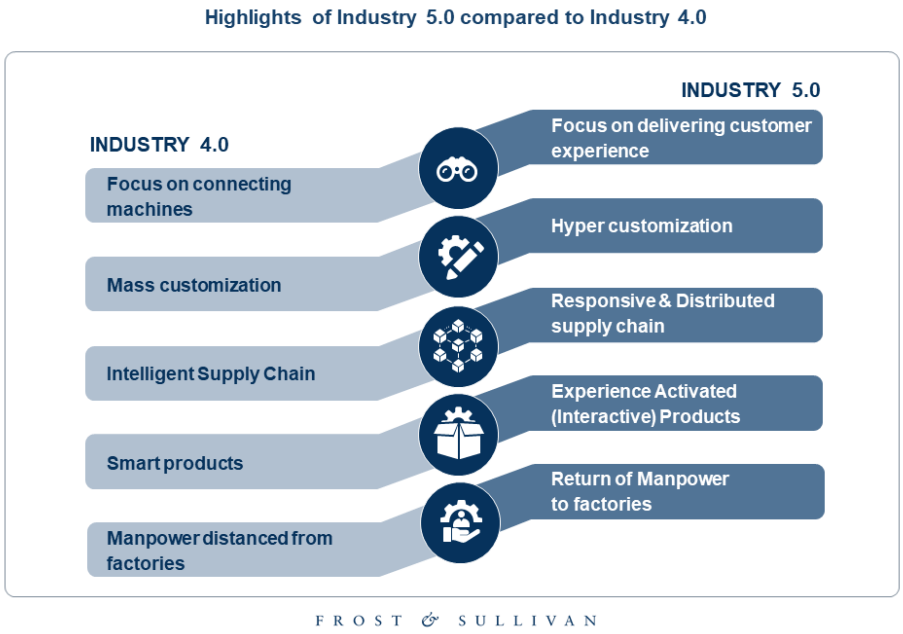
Figure 2.4




Available at https://3433793.fs1.hubspotusercontent-na1.net/hub/3433793/hubfs/202211-Proaction-5-industrial-revolutions-EN.png?width=800&height=514&name=202211-Proaction-5-industrial-revolutions-EN.png

Industry 4.0 introduced a major transformation in the way we 'produce and consume goods and services it is characterised by the use of advanced technologies such as internet of Things (IoT), artificial intelligence (AI) and big data analytics' (Nair, 2023). Industry 5.0 builds upon these foundations integrating humans into the loop.

Figure 2.5




Available at https://www.frost.com/wp-content/uploads/2019/11/Exhibit_1.png

The chatbot embodied Industry 5.0's emphasis on collaboration, offering a personalised experience and an interactive way for users to engage with the platform. The chatbot was created with JavaScript at the core and with guidance and inspiration from codewithfaraz: 'Create Your Own Chatbot with HTML, CSS and Javascript. The chatbot allows users to ask questions based on content related to online safety and data privacy as well as related issues presented on My Digital Compass.

The chatbot operates by referencing the userMessage array. This array contains potential keywords and phrases users might input. (see figure 2.6 for code related to the chatbot).

Figure 2.6

```
const userMessage = [
    ["hi", "hey", "hello"],
    ["online safety"],
```

The botReply contains an array of potential chatbot replies which are linked to the keywords in userMessage. When the user inputs a message, a response is selected from the botReply list.

```
const botReply = [
    ["Hello!", "Hi!", "Hey!", "Hi there!"],
    ["our website will teach you about online safety, do you want the section
for kids, teens or adults " ],
```

An array of fallback responses was also included so that the user would always receive some form of reply even if the bot could not provide a specific answer.

```
  const alternative = [

    "Ask something else...",
    "Hey, I'm listening...",
    "I don't have the answer to that yet...."
  ];
```

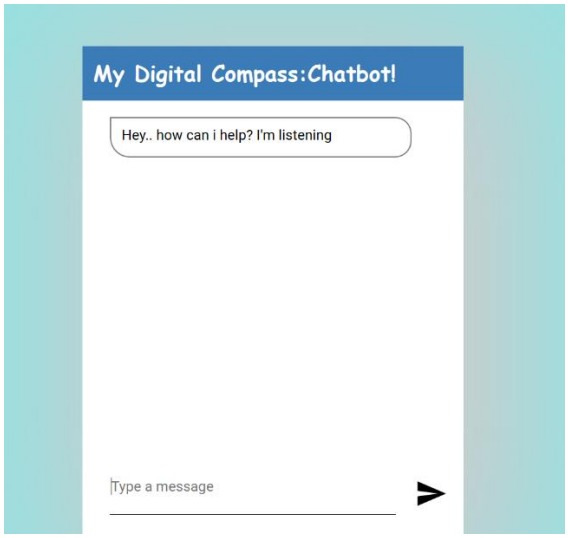
To enhance accessibility, the voiceControl(string) function was included. This leverages the SpeechSynthesis API to give the chatbot a voice, benefiting users who prefer auditory learning or may have difficulty reading ultimately catering to various learning styles.

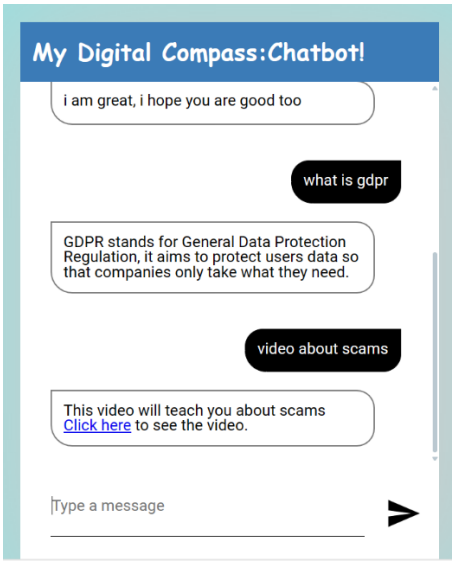
```
function voiceControl(string) {
    let u = new SpeechSynthesisUtterance(string);
    u.text = string;
    u.lang = "en-aus";
    u.volume = 1;
    u.rate = 1;
    u.pitch = 1;
    synth.speak(u);
  }
```

Once the user inputs a message it is converted to lowercase letters, this cleans up the data and ensures that a match is still possible even with capitalisation differences. Users receive responses containing definitions, links to relevant HTML pages for deeper exploration and even links to helpful MP4 videos. The aim of the chatbot is to provide quick answers alongside multiple avenues for further learning.

The front-end architecture of the chatbot was created using HTML and styled with CSS. The interface favoured a clean and simple design with a white background A label was included on the chatbot so that users knew exactly what they were interacting with. The blue colour scheme aligns with the rest of the website this ensures that each element is integrated seamlessly throughout the website.

Figure 2.7



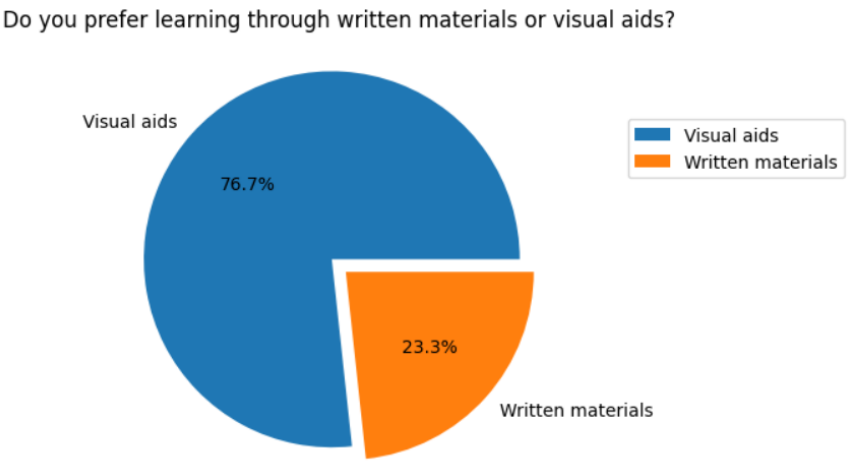




The chatbots interface as seen in figure 2.7. The first image is what you are presented with when you enter the page, while the second image demonstrates sample user interactions and the chatbots responses.

**Infographics and Posters**

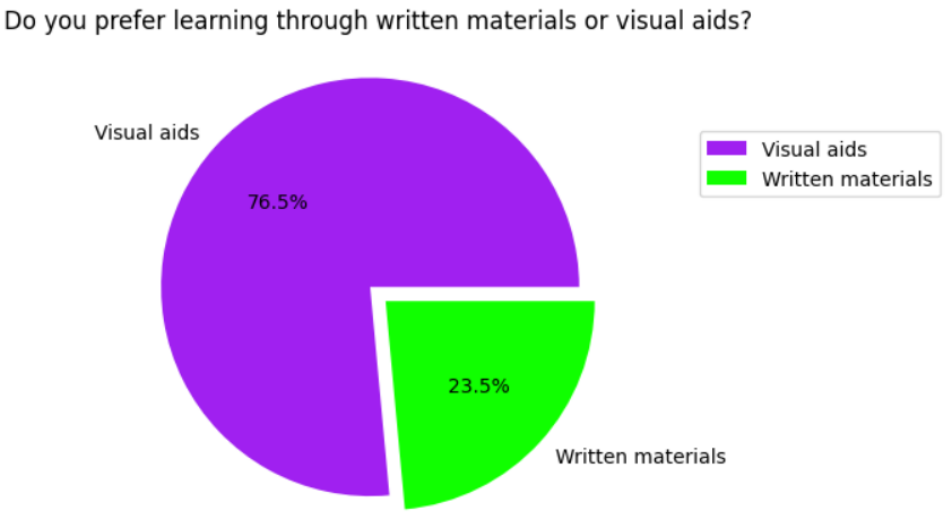
Visual elements were at the core focus on my Digital platform. As discovered from the survey results all respondents preferred to learn visually:

Figure 2.8




Adult survey: ‘Do you prefer learning through written materials or visuals aids?’.

2.9




Teen survey: ‘Do you prefer learning through written materials or visual aids?’.

Both age groups exhibited a strong preference for visual learning aids. A substantial 76.7% of adults and a very similar 76.5% of teenagers reported favouring images, infographics, and videos for learning ( see figure 2.8 & 2.9).

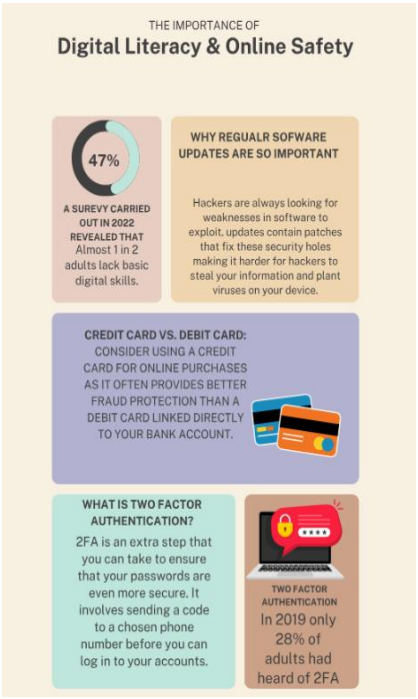
Canva was used to create visually engaging posters and infographics. As respondents from the survey stated how they preferred visual aids it was important to incorporate as many visual elements onto the platform as possible. Canva provides several different themes and designs making it an excellent tool for creating posters and infographics. Canva posters are highly customisable, full creative control is handed over to the user, elements like images, text boxes, graphs and even stats can be added to posters.

The posters contained clear and concise information along with straightforward language to ensure users can understand the key points quickly and easily. Each poster contained relevant age- appropriate content customised to suit the needs of each demographic.

Infographics were created to highlight key issues and essential points about online safety. ‘Visuals are processed 60000 times faster in the brain than text alone…visual aids in the classroom improve learning by up to 400%’ (Parveen, 2020), highlighting how visuals can significantly improve learning.

Figure 3.0



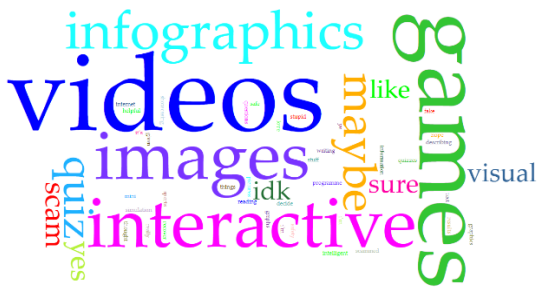



Sample infographics from My Digital Compass.

**Videos**

Respondents were asked what features they would like to see on the platform- the word clouds below were generated using Voyant and contains the most relevant answers to the question: 'Are there any specific features or content you would like to see on an online educational platform addressing these topics?'

Figure 3.1




Kids survey- suggestions for features on the platform.


Teen survey- suggestions for features on the platform.

As seen in figure 3.1 survey results showed a strong preference for video resources. To meet this need, helpful YouTube videos were embedded onto the platform. Age-appropriate, informative cartoons were created using Renderforest. Each cartoon contained images, animations, and icons along with text to create a more engaging experience, background

music creates an immersive atmosphere. Videos were developed from scratch using the animation studio (figure 3.2, 3.3).

Figure 3.2

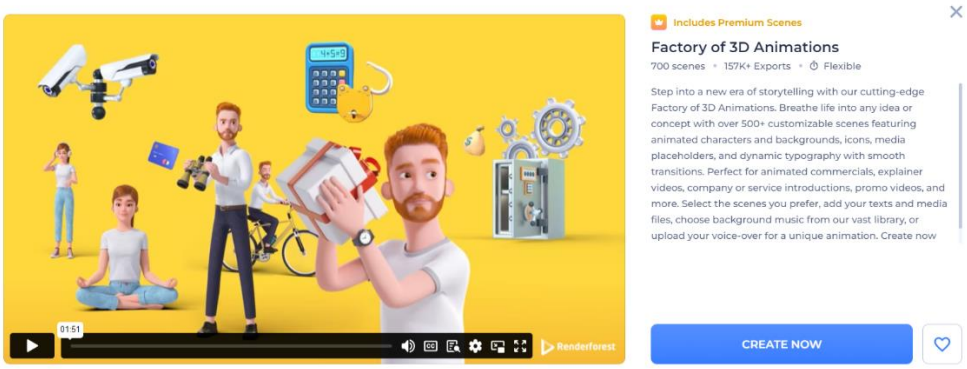
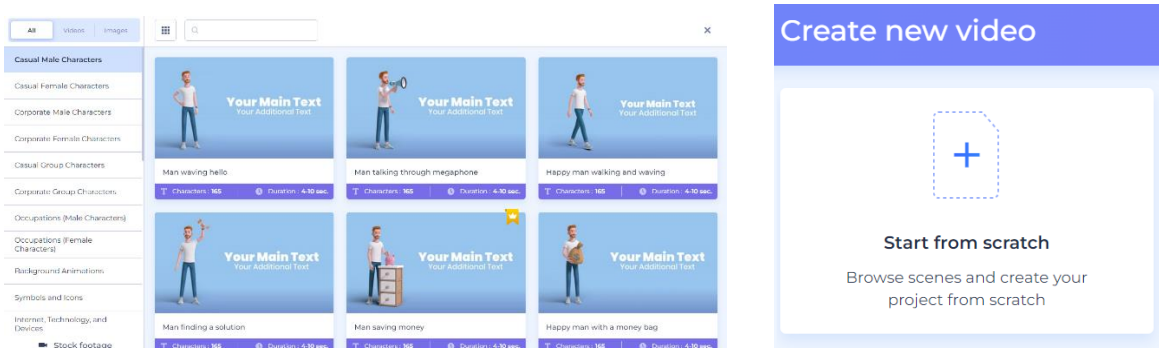
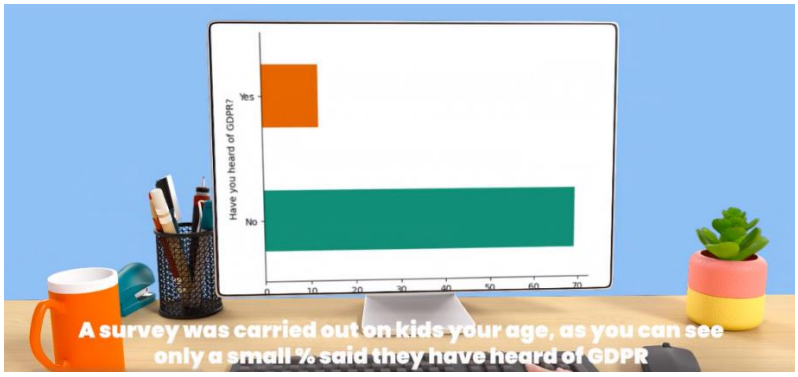



Figure 3.3




Each scene was carefully chosen and contained animations which aligned with each video's topic. Keeping videos to around one-minute prioritised viewer engagement. Renderforest's image integration allowed for survey results to be incorporated directly into the cartoons. Integrating survey results(see figure 3.4) provided additional visual context, allowing viewers to see how their peers responded to certain questions, showcasing survey results reiterates the importance of learning about said topics.

Figure 3.4



## 7. Analysis

The main objective of this project was to identity age-related challenges that people face in relation to online safety and data privacy and uncover how a digital platform can address these challenges, promoting digital literacy for all. As mentioned above the three surveys guided the scope of the project, they provided valuable insights as well as knowledge gaps. The data highlighted age-specific challenges while also revealing broader knowledge gaps common to all age groups.

The platforms design was directly influenced by the survey results, keeping humans at the heart of its creation. This approach aligns with the principles of Industry 5.0, bringing personalisation back into the market; the platform was created based on human input as 'Collaboration among humans and machines' (Adel, 2022) is the core focus of Industry 5.0.

The surveys were made available for 3 weeks via social media, email and text and distributed to local schools to be completed within 2 weeks. The table below provides a breakdown of respondents from each age group:

Table 1.2

| Survey | Respondents | Ages | Gender |
|---|---|---|---|
| Adult Survey | 74 | 18-63 | 56 female, 20 male, 1 non-binary. |
| Teen Survey | 51 | 13-17 | 26 female, 25 male. |
| Kids Survey | 81 | 9-13 | 48 female, 30 male, 3 other. |

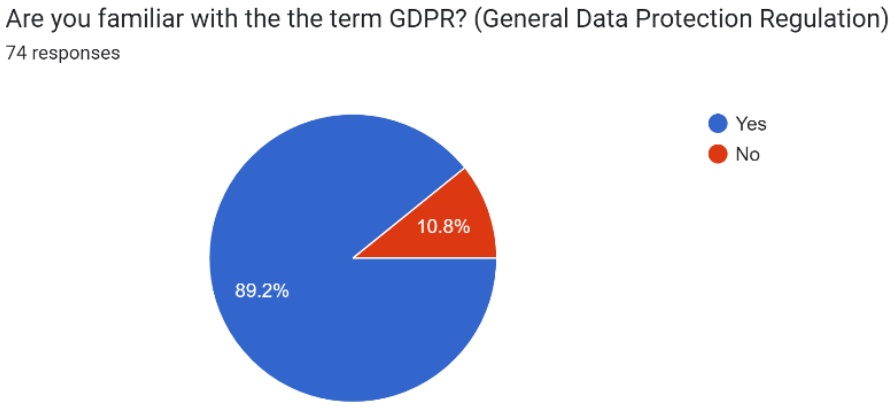
The surveys for kids and teens were distributed to both single-sex and coeducational schools so that a range of educational environments were accessed. As detailed above python pandas were utilised to create graphs and pie charts, allowing for a visual analysis of the survey data.

**Analysis of the data (Key findings)**

The survey data revealed important insights. Importantly it revealed that more educational resources are needed to inform people about online safety, data privacy and the complexities that follow.

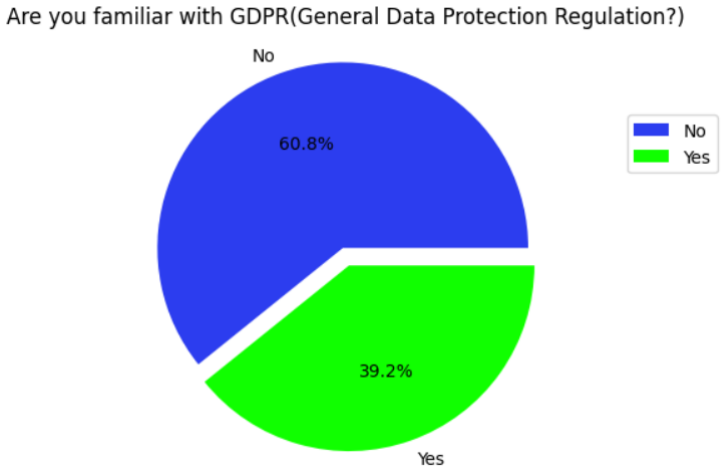
As GDPR is a relatively new concept it was important to include this question in the survey:

Figure 3.5



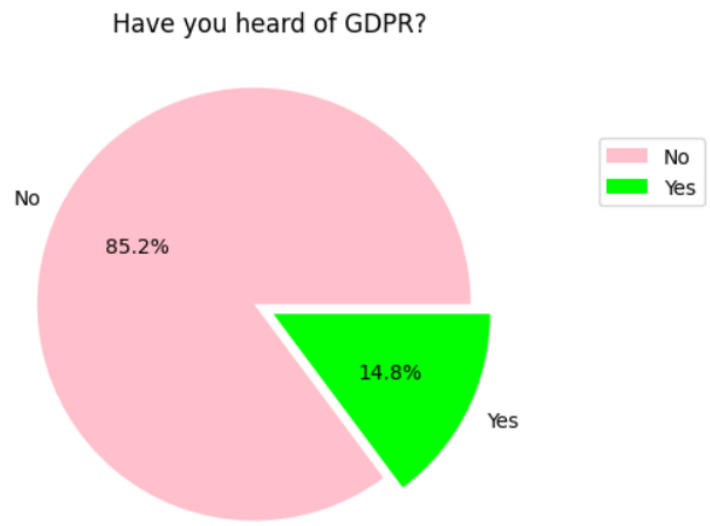

As seen in figure 3.5, the high level of GDPR awareness among adults is encouraging, this suggests potential receptiveness to educational campaigns and initiatives focused on understanding the rights and protections provided by the regulation. While a high percentage of respondents indicated that they had heard of GDPR this figure might overestimate true understanding as the survey only assessed recognition not in-depth knowledge. Evidently it is expected that adults could have more of an understanding of GDPR compared to kids and teenagers.

Figure 3.6




The data reveals a concerning lack of awareness surrounding GDPR among teenagers, with 60.8% of respondents indicating that they have never heard of the regulation (see figure 3.6), suggesting that this demographic may be particularly vulnerable to online privacy risks as they are unsure of their rights regarding data protection. Necessary educational initiatives are needed to empower teenagers about GDPR. A significant majority of both males (17/25) and females (15/26) reported unfamiliarity with the regulation highlighting that both genders exhibit a similar lack of awareness on the topic.

Figure 3.7




Similar to the results from the teens survey a large proportion of kids (85.2%) have never heard of GDPR with only 14.8% of respondents indicating that they are aware of the regulation (see figure 3.7), this could be due to the fact that there are limited child friendly resources out there teaching children about GDPR in an age-appropriate way. These findings underscore the crucial role of both parents and educators in fostering digital literacy and GDPR awareness among young children.

The low level of awareness of GDPR among children (14.8%) reveals a significant gap in educational resources tailored to their needs.

The Data Protection Commission agrees that the rules regarding GDPR are ‘set out in very broad terms’ (DPC, 2021) reinforcing the fact that without sufficient informative resources it is difficult for children and indeed everyone to truly understand the implications of GDPR. It is evident that information ‘must be provided in a concise, transparent, intelligible, and easily accessible form using unique and plain language. The clarity of this information is particularly required where it is being provided to a child’ (DPC, 2021). The Data Protection Commission also reiterate the importance of using ‘non textual measures’ (DPC, 2021) when explaining GDPR.

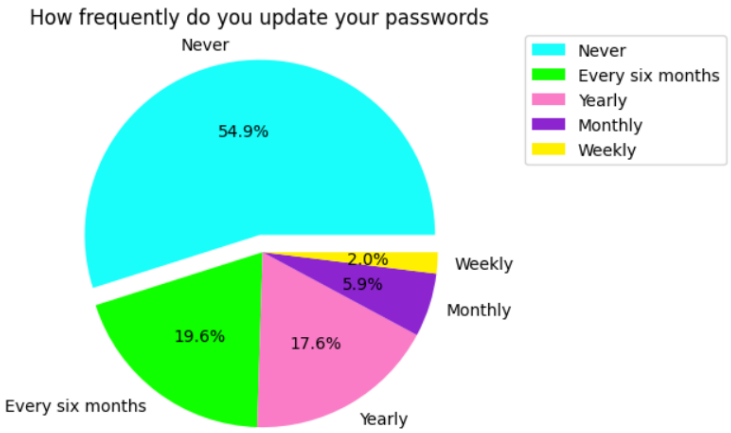
Due to many respondents being unaware of GDPR, it was crucial to investigate any potential connection between data privacy knowledge and password word practices. Therefore, a thorough analysis of password related data was conducted.

From the data gathered it is evident that a large majority of teenagers (54.9%) admit to never changing their passwords, shockingly only 19.6% of respondents change their passwords every six months (see figure 3.8). McAfee recommends changing passwords every 3 months to maximise security, and, in some situations, passwords should be changed more regularly

than this. An interesting trend was observed in relation to passwords, the data revealed that 61.5% (16/26) of females admit to never changing their passwords compared to 44% (11/25) of males. This aligns with research by Juozapavičius et al. (2022) highlighting that 'the password strength of male users consistently exceeds the password strength of female users'. Frequent password changes might contribute to stronger passwords among males, as they gain practice when creating them. Consequently 'male users are more likely to use passwords almost twice as difficult to guess compared with those of female users' (Juozapavičius et al., 2022).

A study carried out by Josephy Bonneau a computer scientist at the University of Cambridge found that 'people over the age of 55 pick passwords double the strength of those chosen by people under 25' (Aron, 2012) perhaps suggesting that older adults are more conscious when it comes to online safety.

Figure 3.8




However, when the same question was analysed in the adult survey it was evident that a higher percentage of adults (71.2%) never change their passwords (see figure 3.9%) with only 1.7% of respondents occasionally changing their passwords. Additionally, adults were also asked if they had received any formal education teaching them how to protect their privacy online (see figure 4.0) shockingly a total of 52.1% said no and 13.7% were unsure; a combined 65.8% of adults lack educational support in this crucial area. This finding aligns with the high percentage of adults who never change passwords, suggesting a potential link between lack of education and poor security practices. Although there was little correlation between GDPR and password practices, one interesting observation was that all participants that answered No to 'Are you familiar GDPR?', the majority answered never to changing passwords with only 1 answering every six months and another answering saying yearly could this point to the fact that people who are unaware of GDPR have bad password practices.

Figure 3.9

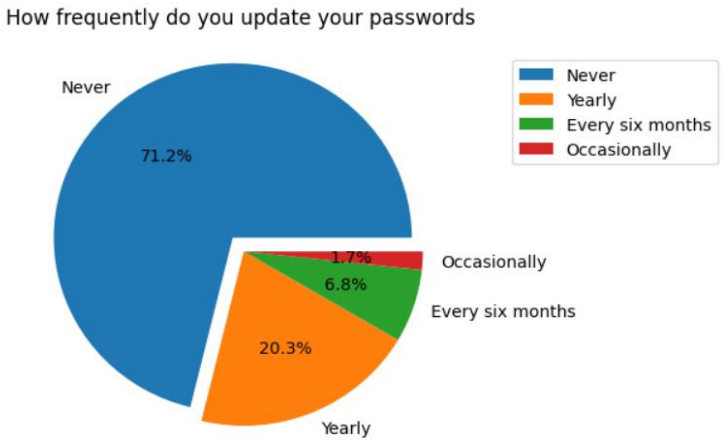
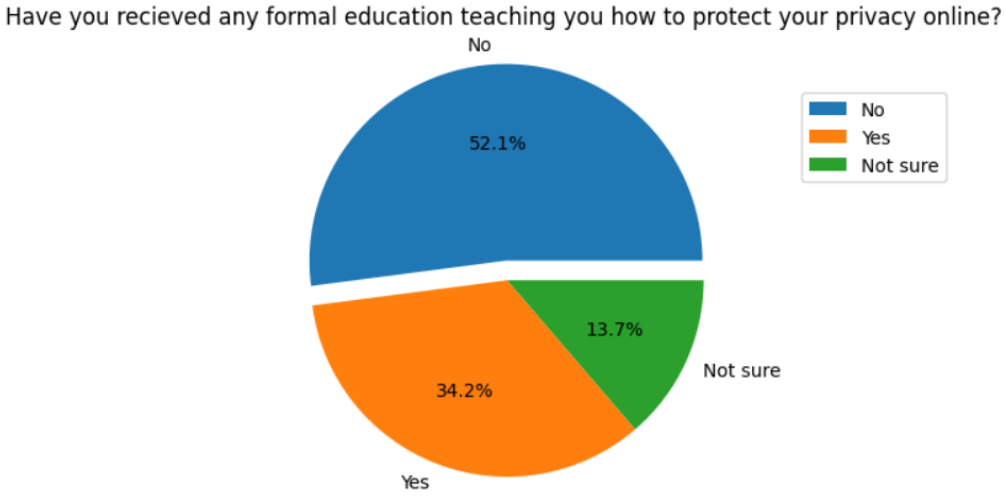



Figure 4.0




A significant concern is revealed by the data: over half (55.6%) of children surveyed in Figure 4.1 were unaware of the minimum age requirement (13 years old) for many social media platforms. Given the increased vulnerability of children to online risks these findings are deeply concerning. This concern is further highlighted by a report from the European Parliament (February 2023) titled 'The Influence of social media on the development of children and young people'. Their findings reveal that '28% of 9–11-year-olds and 63% of 12–14-year-olds use social media daily despite the minimum age of 13 years for most platforms' (European Parliament, 2023). This aligns with results gathered form the surveys where (see figure 4.2) 74/81 of respondents use some form of social media, with a staggering 97.3%. OFCOM, 2022 revealed that 'YouTube was the most- used VSP among all children aged 3-17 for watching videos (83%).

Figure 4.1

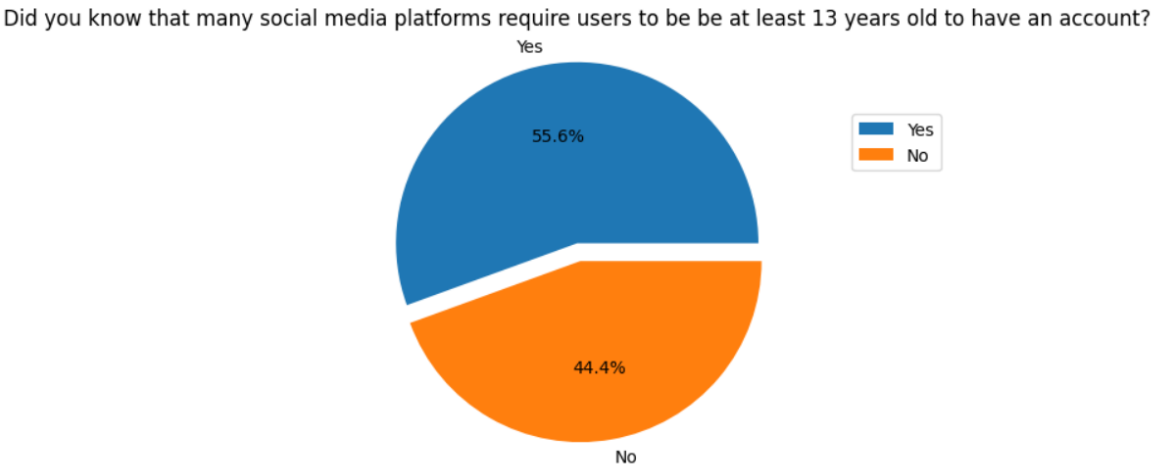
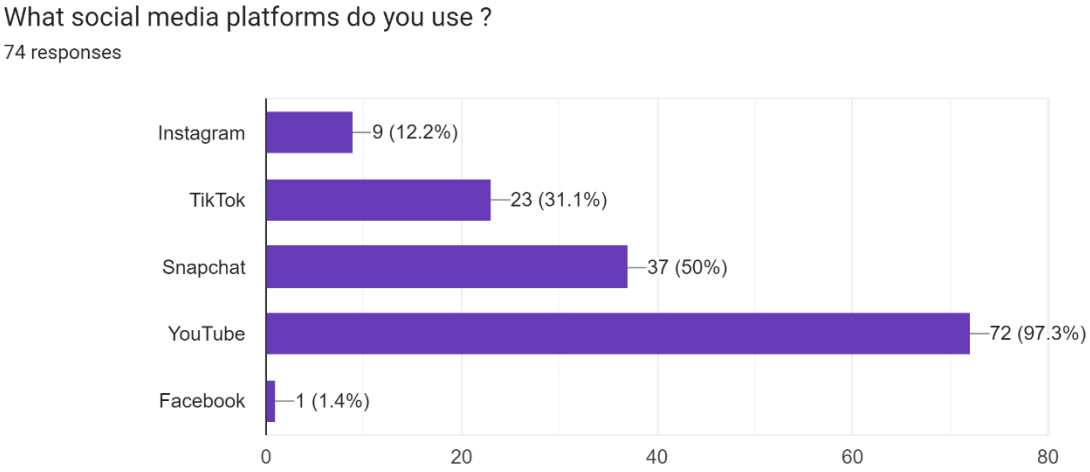



Figure 4.2

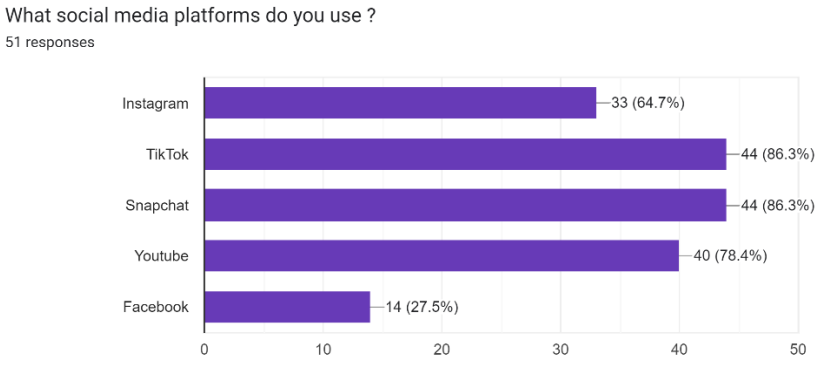



The rise in social media use among younger children might be partly explained by the Covid-19 pandemic. As Bozzola (2022) suggests 'internet usage during Covid-19 allowed communication with peers and school teaching', therefore there was an increase in the use of social media platforms among younger generations. This is consistent with the results of a survey carried out by CyberSafeKids which revealed that at the start of 2020 68% of children had social media platforms, this jumped to 82% at the start of 2021 showcasing the increase in social media among children. The reiterate the idea that despite well-known social media apps such as TikTok and Snapchat 'having a minimum age of 13 this isn't preventing children being active' (RTE, 2021). The popularity of platforms like YouTube and Snapchat reflects a preference for visual and interactive content over text- based platforms like Facebook.

Figure 4.3 supports the idea that teenagers use a wider range of social media platforms compared to younger children. As expected TikTok and Snapchat are the most popular with 86.3% of respondents using these platforms. Only 27.5% of respondents say that they use

Facebook this aligns with research carried out by Vogels, Gelles-Watnick and Massarat (2022) who found that 'TikTok has rocketed in popularity... and is now a top social media platform for teens... with 16% of teens saying that they use it all the time'. TikTok's popularity might be fuelling short-video addiction (SVA) among teenagers, highlighting the platforms potentially addictive design. Supporting this concern, a survey by Chao et al. 2023 found that 85.2% (1147 participants) reported using video platforms. Notably their findings suggest a correlation between heavy video use (Short-video addiction) and poorer mental health as well as both challenges in both school and family environments. This effect was more pronounced for heavy users compared to non-users and moderate users. Recognising that these types of platforms are addictive is the first step in the right direction. Subsequently there has been a drop in the amount of teenagers using Facebook which was also observed in the kid's survey- 'the share of teens who say they use Facebook a dominant social media platform among teens in the centre's 2014-2015 survey has plummeted from 71% then to 32% today' (Vogels, Gelles-Watnick and Massarat, 2022).

Figure 4.3




Qualitative analysis was essential to this research offering richer insights and capturing the real-word experiences of users. This approach complemented quantitative data providing a more comprehensive understanding to address the research question. For instance, when determining desired features for the 'My Digital Compass' platform, qualitative analysis was key.

Aligning with the popularity of TikTok and YouTube among children and teenagers it was no surprise that videos were ranked as the most desired feature for the My Digital Compass platform. Initial attempts to analyse the qualitative data using python pandas encountered difficulties due to the large volume of responses (figure 4.4). Pie charts proved ineffective in handling this extensive dataset. To overcome this challenge Voyant was used to represent the qualitative data. While Voyant may not extract precise percentages, it effectively visualises

recuring themes and provides a clear overall picture of the collected feedback (figure 4.5- details the top feature recommendations received from teenagers for the platform).

Figure 4.4

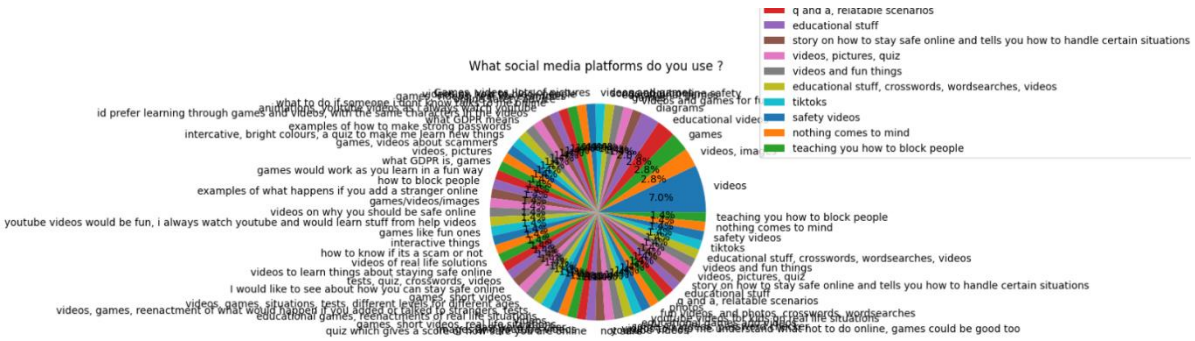
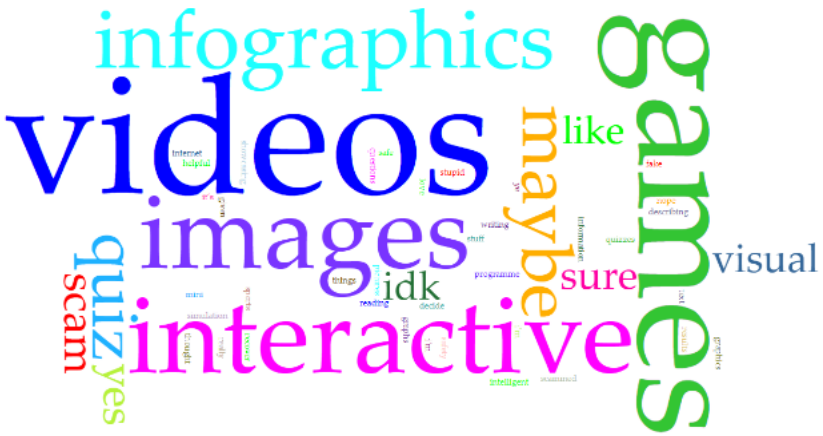



Figure 4.5



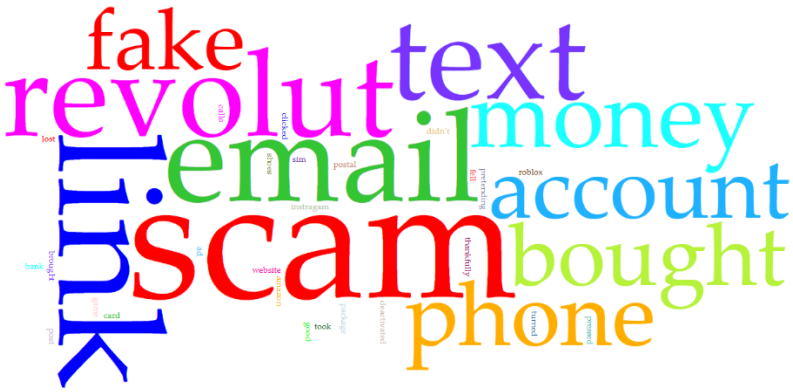

with the rise in phishing scams in recent years it was important to understand what types of scams people are falling for so that sufficient educational resources could be altered to fit the narrative.

When analysing the data it was evident that adults and teenagers are susceptible to phishing scams, although both demographics fall for similar scams some noticeable differences can be observed (see figures 4.6 & 4.7). A survey conducted in 2019 by the Banking and Payments Federation Ireland revealed that older Irish adults are ‘losing almost six times more money to scammers than younger generations’ (BPFI, 2019), while this data may not be the most recent, its relevance persists. The BPFI survey revealed that older people ‘are most likely to be targeted via email’ (BPFI, 2019), this aligns with the fact that the results of the adult survey uncovered that adults have fallen for email-based bank scams. The fact that people are still falling for the same scams five years after the BPFI report highlights the ongoing threat. With advancements in technology and increasingly sophisticated scams addressing this knowledge gap is crucial for improving online safety and awareness.

Evidently, adults are more likely to fall for bank and credit card scams because they typically manage more complex financial accounts and transactions. Teenagers may be less vigilant about banking related scams, as their account may be managed by parents or guardians reducing their sense of responsibly however this isn't always a positive thing but was observed from the data.

Figure 4.6


Figure 4.7




Teenagers are particularly vulnerable to scams spread via text message and on social media platforms like Instagram. Scammers exploit the popularity of social media among teens often using these platforms to impersonate trusted brands to gain access to personal information and bank details.

The platforms design was strongly influenced by survey insights; however, the overrepresentation of female respondents suggests a potential bias and the need for further research with a more balanced gender distribution. Despite efforts to recruit male participants female respondents demonstrated greater enthusiasm potentially suggesting that females prioritise safety concerns.

**Artefact Analysis**

**Addressing the research question: (The websites functionality)**

The artefact effectively addressed the research question, '**What are the key challenges faced by users of different age groups regarding online safety and data privacy and how can a digital platform address these challenges?'.** The surveys, literature review and environmental scan set out to discover the range of different challenges faced by each demographic. These findings informed the creation of a versatile digital platform offering users a variety of different ways to learn and explore online safety and data privacy. The platform distinguished itself through interactive features including a chatbot and knowledge quiz providing an engaging experience for all users. The project firmly embodies the principles of Industry 5.0 by prioritising human needs and experiences throughout the design process. The platform tackles the key online safety challenges faced by each age group ensuring that a variety of learning styles are accommodated. The open day provided valuable user insights. After a brief demonstration of the artefact, participants explored the platform independently and expressed positive feedback. Overall they found it to be a highly informative resource expressing how the convenience of having all materials for all age groups in one place was a significant benefit. One participant in particular stated that it would be a useful platform as they can learn about information relevant to their age group alongside their children resulting in effective collaborative learning. The chatbot received particular interest from users, they enjoyed the fact that it was able to speak the answers received and felt that it would be a great way to quickly navigate the platform.

**Limitations of the artefact:**

Hand coding the platform using HTML, CSS and JavaScript proved both rewarding and challenging. While it offered complete creative control, the process was time consuming, particularly when refining element placement, meticulous planning was required throughout to ensure that that each element was seamlessly integrated onto the platform. Utilising a Content Management System (CMS) could have expediated development however this may have limited the platforms functionality and its ability to seamlessly integrate some of the custom features that were chosen for the platform (chatbot, knowledge quiz).

Currently the platform is designed primarily for viewing on laptops and desktop computers. Time constraints prevented the implementation of responsive design limiting the platforms accessibility on certain devices. With additional development time, the platform could be optimised to function seamlessly on any device, significantly expanding its reach.

While hand-coding the digital artefact effectively served the projects current scope, expansion would demand more efficient development approaches. For a larger-scale platform a CMS would be essential for sustainability.

**What was learned?**

This project involved a significant learning curve, including the acquisition of JavaScript and a comprehensive review of HTML and CSS. Understanding JavaScript was crucial as it was used to create interactive elements on My Digital Compass. Online resources were utilised to understand the core concepts behind JavaScript, many books were also attained from the UCC library including; The essential guide to HTML 5, Learn PHP 8, JavaScript for Web Developers and Practical Web Development: Learn CSS, JavaScript, PHP, and more with this vital guide to modern web development, were among some of the most helpful resources which provided me with the necessary insights into JavaScript.

Overall, this research project relied heavily on the survey results to create a user-centric platform. The data collected revealed the real-world experiences and needs of different age groups. A thorough in-depth analysis proved instrumental in addressing the research question effectively.

## 8. Conclusion

This project delved into the challenges that different age groups face when navigating the internet. The research question 'What are the key challenges faced by users of different age groups regarding online safety and data privacy and how can a digital platform address these issues?' guided the development of 'My Digital Compass'. Three surveys, a through literature review and an environmental scan provided extremely useful insights and laid the groundwork out for the platform.

Findings from the surveys revealed that a large proportion of society are unaware of GDPR, don't practice password hygiene and require additional help when it comes to learning about online safety, data privacy and related topics, a significant number of children under the age of 13 use social media platforms, research has suggested that this number has risen significantly since Covid-19. Teenagers were asked to share their feelings about the online safety education they have received so far, while a few positive comments were noted the overwhelming majority of responses expressed a lack of adequate support. Answers such as 'I don't get much help from school', 'it hasn't been very helpful' and 'I haven't received any education in this regard' reveal a concerning dissatisfaction with existing resources. Some even stated that they couldn't recall learning about online safety at all. This highlighted the urgent need for more impactful educational initiatives designed to resonate with teenagers and provide them with essential memorable knowledge on this topic.

Just as teenagers expressed dissatisfaction with current educational initiatives a similar lack of support was evident in the adult survey. A staggering 65.8% of adults lack sufficient educational support in relation to online safety etc. This likely stems from the fact that they did not grow up immersed in technology like younger generations therefore did not learn about technological complexities in school. This alarming statistic highlighted the need for an educational platform targeting older adults.

When asked 'Who teaches you how to be safe online?' children listed family members, teachers and school workshops, this revealed a crucial point; no one mentioned learning from online sources or educational platforms, this suggested a significant gap in the availability of engaging and accessible online safety resources designed for young learners.

The expressed uncertainly about online safety and data privacy across all age groups highlighted the need for a new approach that addresses these issues in ways which resonate with people. As people become more reliant on technology and social media it is evident that it has the potential to shorten our attention spans, 'one study has shown that over reliance on technology has shortened our attention span from twelve minutes to five minutes' (Cundiff, 2021). Therefore, in order to combat this a variety of visual elements were incorporated onto the platform to ensure that people would retain the information better.

Drawing from inspiration from Industry 5,0's human centric approach the platform was designed with insights gained from in-depth user surveys. These surveys revealed that a one size fits all approach to online safety education is ineffective highlighting the need for different solutions across age groups. The platform incorporated interactive elements like quizzes, adaptive explainer videos and a supportive chatbot with Industry 5.0's goal of empowering individuals through technology. These features promote active learning and encourage users to take back control.

Due to the projects timeline certain desired features could not be fully implemented. Ideally the chatbot would have been implemented using a robust server-side solution like XAMMP and phpMyAdmin. This would have allowed for more complex database interactions, enabling the chatbot to handle a broader range of potential user inputs and a variety of different unique answers. The chatbot's reliance on JavaScript limited its flexibility. Each potential question and response had to be manually coded, integrating a database would streamline this process making it easier to expand the chatbots knowledge base. However, this is not to say that this route will not be implemented in the future, this will definitely be considered as the next step to improve the platform.

While this project focused on three core demographics- children, teens, and adults- the broad adult category could be further refined. Given more time it would have been beneficial to create distinct sections for young adults, adults and older adults recognising that each of these groups also face unique challenges online. As when carrying out research it was evident that a 20-year-old adult would face different challenges to a 70-year-old adult. However, due to the time constraints, the project focused on addressing adults as a whole.

A key future objective would be to translate the platform into multiple languages. This would broaden its reach making it accessible to a global audience. Valuable insights could be gathered from user data across different cultures and countries. As My Digital Compass evolves thoughtful design aligned with Industry 5.0's values is essential. As more AI related elements are integrated onto the platform data privacy and responsible algorithm development must be at the forefront. This includes ensuring transparency for users about how their information is used.

Overall, the 'My Digital Compass' platform effectively addresses the core research question, highlighting the distinct online safety and data privacy challenges faced by different age groups. While technology poses challenges, this project highlights its potential to combat the various issues faced by different age groups through innovative educational resources.

# Reference list

Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N. and Schaub, F. (2017). Nudges for

Privacy and Security. *ACM Computing Surveys*, 50(3), pp.1–41. doi:https://doi.org/10.1145/3054926.

Adel, A. (2022). Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas. *Journal of Cloud Computing*, [online] 11(1). doi:https://doi.org/10.1186/s13677-022-00314-5.

Akundi, A., Euresti, D., Luna, S., Ankobiah, W., Lopes, A. and Edinbarough, I. (2022). State of Industry 5.0—Analysis and Identification of Current Research Trends. *Applied System Innovation*, [online] 5(1), p.27. doi:https://doi.org/10.3390/asi5010027.

Alagood, J., Prybutok, G. and Prybutok, V.R. (2023). Navigating Privacy and Data Safety: The Implications of Increased Online Activity among Older Adults Post-COVID-19 Induced Isolation. *Information*, [online] 14(6), p.346. doi:https://doi.org/10.3390/info14060346.

Arachchilage, N.A.G. and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, [online] 38, pp.304–312. doi:https://doi.org/10.1016/j.chb.2014.05.046.

arimetrics.com. (2023). *What is FileZilla | Definition, uses and uploads of files*. [online] Available at: https://www.arimetrics.com/en/digital-glossary/filezilla.

Aron, J. (2012). Passwords for over-55s are twice as secure as those chosen by teenagers. *New Scientist*, 214(2866), p.22. doi:https://doi.org/10.1016/s0262-4079(12)61347-5.

Barnardos. (n.d.). *Online Safety Programme*. [online] Available at: https://www.barnardos.ie/learning-development/training/online-safety-programme/ [Accessed 26 Apr. 2024].

Bawden, D., 2008. Origins and concepts of digital literacy. *Digital literacies: Concepts, policies and practices*, *30*(2008), pp.17-32.

Bozzola, E. (2022). The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks. *International Journal of Environmental Research and Public Health*, [online] 19(16), p.9960. doi:https://doi.org/10.3390/ijerph19169960.

bpfi (2019). *Older Irish people losing almost six times more money to scammers than younger generation – FraudSMART Survey*. [online] Banking & Payments Federation

Ireland. Available at: https://bpfi.ie/older-irish-people-losing-almost-six-times-money-scammers-younger-generation-fraudsmart-survey/ [Accessed 13 Nov. 2023].

Bravo, F. (2019). *Why I don't use Wordpress and why you shouldn't either*. [online] www.linkedin.com. Available at: https://www.linkedin.com/pulse/why-i-dont-use-wordpress-you-shouldnt-either-frank-bravo/ [Accessed 19 Apr. 2024].

Burke, J. (2023). *Why and how to use Google Colab | TechTarget*. [online] Enterprise AI. Available at: https://www.techtarget.com/searchenterpriseai/tutorial/Why-and-how-to-use-Google-Colab.

Canva (2024). *Canva*. [online] Canva. Available at: https://www.canva.com/.

Chaduneli, M. and Saxena, R. (n.d.). *Do digital natives value their online privacy? – Network Readiness Index*. [online] networkreadinessindex.org. Available at: https://networkreadinessindex.org/do-digital-natives-value-their-online-privacy/#:~:text=As%20digital%20natives%20are%20increasingly [Accessed 23 Apr. 2024].

Chao, M., Lei, J., He, R., Jiang, Y. and Yang, H. (2023). TikTok use and psychosocial factors among adolescents: Comparisons of non-users, moderate users, and addictive users. *Psychiatry Research*, 325, p.115247. doi:https://doi.org/10.1016/j.psychres.2023.115247.

Cundiff, J. (2021). *Is technology causing our attention-span to shrink?* [online] Epigram. Available at: https://epigram.org.uk/is-technology-causing-our-attention-span-to-shrink/.

CyberSafeKids (n.d.). *Homepage*. [online] CyberSafeKids. Available at: https://www.cybersafekids.ie/.

Data Protection Commission (2021). *CHILDREN FRONT AND CENTRE FOR A CHILD-ORIENTED APPROACH TO DATA PROCESSING FUNDAMENTALS*. [online] Available at: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf.

Faraz (2023). *Create Your Own Chatbot with HTML, CSS, and JavaScript (Source code)*. [online] Code with Faraz - Best Front-End Components and Blogs. Available at:

https://www.codewithfaraz.com/content/133/create-your-own-chatbot-with-html-css-and-javascript [Accessed 20 March. 2024].

Fitzgerald, A. (2024). *10 Best Blue Websites in 2022 [+ Their Color Schemes]*. [online] blog.hubspot.com. Available at: https://blog.hubspot.com/website/blue-website#:~:text=Incorporating%20blue%20into%20your%20website.

Gingerich, M. (2018). *What is RenderForest and How Can You Use It for Business?* [online] Mike Gingerich. Available at: https://www.mikegingerich.com/blog/renderforest-business/.

Hagen, J. and Lysne, O. (2016). Protecting the digitized society—the challenge of balancing surveillance and privacy. *The Cyber Defense Review*, [online] 1(1), pp.75–90. Available at: https://www.jstor.org/stable/26267300.

Herrle, J. and Hirsh , J. (2019). *The Peril and Potential of the GDPR*. [online] Centre for International Governance Innovation. Available at: https://www.cigionline.org/articles/peril-and-potential-gdpr/?utm_source=google_ads&utm_medium=grant&gclid=CjwKCAiAiKuOBhBQEiwAId_sKx4DwmFRkN1d0lTnx2j1sbjytYgf5vVu5QJeRnvgXOT8WIRxGPf63xoCPlMQAvD_BwE.

INTERNET MATTERS (2014). *Internet Matters*. [online] Internet Matters. Available at: https://www.internetmatters.org/.

Ioannou, A., Tussyadiah, I. and Miller, G. (2020). That's Private! Understanding Travelers' Privacy Concerns and Online Data Disclosure. *Journal of Travel Research*, p.004728752095164. doi:https://doi.org/10.1177/0047287520951642.

Ivan, L. and Fernández-Ardèvol, M. (2017). Older people and the use of ICTs to communicate with children and grandchildren. *Transnational Social Review*, 7(1), pp.41–55. doi:https://doi.org/10.1080/21931674.2016.1277861.

Ivan, Loredana & Fernández-Ardèvol, Mireia. (2017). Older people and the use of ICTs to communicate with children and grandchildren. Transnational Social Review. 7. 1-15. 10.1080/21931674.2016.1277861.

Jacob Aron (2012). *Over-55s pick passwords twice as secure as teenagers'*. [online] New Scientist. Available at: https://www.newscientist.com/article/dn21871-over-55s-pick-passwords-twice-as-secure-as-teenagers/.

Jiang, Mengtian & Tsai, Hsin-yi & Cotten, Shelia & Rifon, Nora & Larose, Robert & Alhabash, Saleem. (2016). Generational Differences in Online Safety Perceptions, Knowledge, and Practices. Educational Gerontology. 42. 10.1080/03601277.2016.1205408.

Johann Čas, Bellanova, R., J. Peter Burgess, Friedewald, M. and Peissl, W. (2017). Introduction. *Routledge eBooks*, pp.1–12. doi:https://doi.org/10.4324/9781315619309-1.

Juozapavičius, A., Brilingaitė, A., Bukauskas, L. and Lugo, R.G. (2022). Age and Gender Impact on Password Hygiene. *Applied Sciences*, 12(2), p.894. doi:https://doi.org/10.3390/app12020894.

Lindner, J. (2023). *Must-Know Internet Dangers Statistics [Latest Report] • Gitnux*. [online] gitnux.org. Available at: https://gitnux.org/internet-dangers-statistics/#:~:text=53%25%20of%20internet%20users%20are%20concerned%20about%20protecting%20their%20privacy%20online.&text=by%20cyberbullying%2C%20and-.

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019). *Children's Data and Privacy Online Growing up in a Digital Age an Evidence Review*. [online] Available at: https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf.

Lyon, D. and Zureik, E. (1996). *Computers, Surveillance, and Privacy*. [online] *Google Books*. University of Minnesota Press. Available at: https://books.google.ie/books/about/Computers_Surveillance_and_Privacy.html?id=7eJzQgAACAAJ&redir_esc=y [Accessed 26 Apr. 2024].

Mckinney, W. (2013). *Python for data analysis*. Beijing: O'reilly.

McPherson, L. (2019). *Survey Maker Showdown: Google Forms vs. Survey Monkey*. [online] Zapier. Available at: https://zapier.com/blog/google-forms-vs-surveymonkey/.

Meyer, J. (2023). *The Essential Guide to HTML5*. *Apress eBooks*. doi:https://doi.org/10.1007/978-1-4842-8722-4.

Microsoft (2024). *Visual Studio Code*. [online] Visualstudio.com. Available at: https://code.visualstudio.com/.

Nair, S. (26AD). *Industry 4.0 vs. Industry 5.0: The Key Differences*. [online] www.linkedin.com. Available at: https://www.linkedin.com/pulse/industry-40-vs-50-key-differences-syam-nair/.

Nyst, C. and Falchetta, T. (2017). The Right to Privacy in the Digital Age. *Journal of Human Rights Practice*, 9(1), pp.104–118. doi:https://doi.org/10.1093/jhuman/huw026.

O'Callaghan, C., Gorato, L. and McHugh, D. (n.d.). *Industry 5.0 -Everything to Know*. [online] innopharmatechnology. Available at: https://www.innopharmatechnology.com/news/what-is-industry-5-0#:~:text=What%20is%20Industry%205.0%3F [Accessed 22 Apr. 2024].

OFCOM (2023). *Children and Parents: Media Use and Attitudes*. [online] *Ofcom*. OFCOM. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf.

Parveen, Akthar & Husain, Naushad. (2021). INFOGRAPHICS AS A PROMISING TOOL FOR TEACHING AND LEARNING.

P. Romansky, R. and S. Noninska, I. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17(5), pp.5288–5303.

ParadiseLostTutorial (n.d.). *Text Analysis 101: Voyant introduction*. [online] Available at: https://library.villanova.edu/application/files/9815/8739/5480/VoyantToolsParadiseLostTutorial.pdf.

paula (2022). *What is Industry 5.0? New Wave of Industrial Digitization*. [online] Stefanini. Available at: https://stefanini.com/en/insights/news/what-is-industry-50-how-shifting-objectives-enables-transformation.

Pedersen, S. (2013). UK young adults' safety awareness online – is it a 'girl thing'?. *Journal of Youth Studies*, 16(3), pp.404–419. doi:https://doi.org/10.1080/13676261.2012.710741.

PHP (2019). *PHP: What is PHP? - Manual*. [online] Php.net. Available at: https://www.php.net/manual/en/intro-whatis.php.

Prettyman, S. (2020). *Learn PHP 8*. *Apress eBooks*. doi:https://doi.org/10.1007/978-1-4842-6240-5.

Prince, C., Nessrine Omrani and Schiavone, F. (2024). Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe. *Information Technology & People*, 37(8), pp.1–24. doi:https://doi.org/10.1108/itp-05-2023-0467.

Purnama, S., Ulfah, M., Machali, I., Wibowo, A. and Narmaditya, B.S. (2021). Does digital literacy influence students' online risk? Evidence from Covid-19. *Heliyon*, 7(6), p.e07406. doi:https://doi.org/10.1016/j.heliyon.2021.e07406.

Reym, M.V.D. (2020). *7 Advantages of Using Google Colab for Python*. [online] Medium. Available at: https://python.plainenglish.io/7-advantages-of-using-google-colab-for-python-82ac5166fd4b.

Rushda, S. (2024). *Industry 5.0: Connecting Humans and Technology for Sustainable Growth*. [online] HGS. Available at: https://hgs.cx/blog/industry-5-0-connecting-humans-and-technology-for-sustainable-growth/ [Accessed 25 Apr. 2024].

Sadhir, M., Stockburger, S. and Omar, H. (n.d.). *Challenges of Internet and Social Media Use in Adolescents Challenges of Internet and Social Media Use in Adolescents*. [online] Available at: https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1233&context=pediatrics_facpub.

seaborn.pydata.org. (n.d.). *An introduction to seaborn — seaborn 0.12.1 documentation*. [online] Available at: https://seaborn.pydata.org/tutorial/introduction.html.

sharathchandark (2024). *Password Validation Check in HTML CSS & JavaScript | Show Hide Password Toggle*. [online] Medium. Available at: https://medium.com/@sharathchandark/password-validation-check-in-html-css-javascript-show-hide-password-toggle-c57ebde8eb8e [Accessed 03 March. 2024].

Sharples, Mike & Graber, Rebecca & Harrison, Colin & Logan, Kit. (2009). E-safety and Web 2.0 for children aged 11-16. J. Comp. Assisted Learning. 25. 70-84.

Simon, M. (2023). *JavaScript for Web Developers*. *Apress eBooks*. doi:https://doi.org/10.1007/978-1-4842-9774-2.

Slay Studios . (2023). *hand coded vs wordpress website April 13, 2023*. [online] Available at: https://slaystudios.com.my/hand-coded-vs-wordpress-website/ [Accessed 19 Apr. 2024].

Social media use among children surges during lockdown. (2021). *www.rte.ie*. [online] Available at: https://www.rte.ie/news/2021/0209/1196092-safety-online/.

Soyoof, A., Barry Lee Reynolds, Neumann, M.M., Scull, J., Tour, E. and McLay, K. (2023). The impact of parent mediation on young children's home digital literacy practices and learning: A narrative review. *Journal of Computer Assisted Learning*. doi:https://doi.org/10.1111/jcal.12866.

Steele, M. (2021). *Maintaining Your Online Privacy*. [online] NIST. Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/maintaining-your-online-privacy.

Steinfeld, Nili. (2021). Parental mediation of adolescent Internet use: Combining strategies to promote awareness, autonomy and self-regulation in preparing youth for life on the web. Education and Information Technologies. 26. 10.1007/s10639-020-10342-w.

Stoilova, M., Livingstone, S. and Nandagiri, R. (2020). Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy. *Media and Communication*, 8(4), pp.197–207. doi:https://doi.org/10.17645/mac.v8i4.3407.

Supramani, S. (2023). *Bridging Generational Gaps With Technology, How Different Age Groups Are Catching Up With Tech Trends – IIUM in the News*. [online] Available at: https://newsroom.iium.edu.my/index.php/2023/02/14/bridging-generational-gaps-with-technology-how-different-age-groups-are-catching-up-with-tech-trends/.

Tarzana Treatment Centers. (2022). *Study Shows TikTok Addiction and Pathological Dependence in Youth*. [online] Available at: https://www.tarzanatc.org/study-shows-tiktok-addiction-and-pathological-dependence-in-youth/.

Terras, M.M. and Ramsay, J. (2016). Family Digital Literacy Practices and Children's Mobile Phone Use. *Frontiers in Psychology*, 7. doi:https://doi.org/10.3389/fpsyg.2016.01957.

The influence of social media on the development of children and young people STUDY Requested by the CULT Committee Policy Department for Structural and Cohesion Policies Directorate-General for Internal Policies PE EN. (2023). Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/733109/IPOL_STU(2023)733109_EN.pdf.

Thru, Inc. (n.d.). *What Is Secure File Transfer Protocol (SFTP)? A Complete Guide to SFTP*. [online] Available at: https://www.thruinc.com/what-is-sftp-secure-file-transfer-protocol/#:~:text=SFTP%20stands%20for%20SSH%20File [Accessed 19 Apr. 2024].

Tuama, D.Ó. (2022). *What is VS Code? (Visual Studio Code)*. [online] Code Institute Global. Available at: https://codeinstitute.net/ie/blog/what-is-vs-code/ [Accessed 19 Apr. 2024].

Unesco.org. (2018). Available at: https://unesdoc.unesco.org/ark:/48223/pf0000265403.locale=en.

Vespoli, G., Taddei, B., Imbimbo, E., Lisa De Luca and Annalaura Nocentini (2024). The concept of privacy in the digital world according to teenagers. *Zeitschrift für Gesundheitswissenschaften*. doi:https://doi.org/10.1007/s10389-024-02242-x.

Vogels, E.A., Gelles-Watnick, R. and Massarat, N. (2022). *Teens, Social Media and Technology 2022*. [online] Pew Research Center. Available at: https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

W3schools (2019a). *CSS Introduction*. [online] W3schools.com. Available at: https://www.w3schools.com/Css/css_intro.asp.

W3schools (n.d.). *Pandas Introduction*. [online] www.w3schools.com. Available at: https://www.w3schools.com/python/pandas/pandas_intro.asp.

W3schools (2019b). *What is JavaScript*. [online] W3schools.com. Available at: https://www.w3schools.com/whatis/whatis_js.asp.

Waldo, J., Lin, H.S. and Cox, L.H. (2010). Thinking About Privacy: Chapter 1 of 'Engaging Privacy and Information Technology in a Digital Age'. *Journal of Privacy and Confidentiality,* 2(1). doi:https://doi.org/10.29012/jpc.v2i1.581.

Webwise.ie. (2018). *Webwise.ie*. [online] Available at: https://www.webwise.ie/.

Wellens, P 2015, Practical Web Development : Learn CSS, JavaScript, PHP, and More with This Vital Guide to Modern Web Development, Packt Publishing, Limited, Birmingham. Available from: ProQuest Ebook Central. [24 April 2024].

West, S.M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58(1), pp.20–41.

Willsie, T. (2020). *5 Important Reasons Why You Should Not Use WordPress for Your Website*. [online] www.keepsecure.ca. Available at: https://www.keepsecure.ca/blog/5-important-reasons-why-you-should-not-use-wordpress-for-your-website/ [Accessed 19 Apr. 2024].

Yaraghi, N. and Lai, S. (2022). *How the pandemic has exacerbated online privacy threats*. [online] Brookings. Available at: https://www.brookings.edu/articles/how-the-pandemic-has-exacerbated-online-privacy-threats/.

Zaeem, R.N. and Barber, K.S. (2020). The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems*, 12(1), pp.1–20. doi:https://doi.org/10.1145/3389685.

Zapletal, A., Wells, T., Russell, E. and Skinner, M.W. (2023). On the triple exclusion of older adults during COVID-19: Technology, digital literacy and social isolation. *Social Sciences & Humanities Open*, [online] 8(1), p.100511. doi:https://doi.org/10.1016/j.ssaho.2023.100511.

Zeissig, E.-M., Lidynia, C., Vervier, L., Gadeib, A. and Ziefle, M. (2017). Online Privacy Perceptions of Older Adults. *Human Aspects of IT for the Aged Population. Applications, Services and Contexts*, pp.181–200. doi:https://doi.org/10.1007/978-3-319-58536-9_16.

# Appendix

## Survey Questions

### Kids Survey Questions:

1. Age
2. Gender(optional)
3. What social media platforms do you use?
   - Instagram
   - TikTok

- Snapchat
- YouTube
- Facebook

4. Did you know that many social media platforms require users to be at least 13 years old to have an account?
   - Yes
   - No
5. Do you think it's important to learn about online safety?
   - Yes
   - No
6. Name some ways you can stay safe online?
7. Who teaches you how to stay safe online?
8. Have you heard of GDPR?
   - Yes
   - No
9. If someone you don't know tries to be your online friend, what would you do?
10. Would you use a website that teaches you about online safety through images and videos?
    - Yes
    - No
    - Maybe
11. What kind of things would you like to see on the website which helps you learn about the above topics e.g., Educational Games, Images, Videos? Please suggest anything else you would like to see on the website.

**Teenagers Survey Questions:**

1. Age
2. Gender(optional)
3. What social media platforms do you use?
   - Instagram
   - TikTok
   - Snapchat
   - YouTube
   - Facebook
4. How do you feel about the online safety education you have received so far? What have you found most helpful?
5. Have you ever fallen for a scam?
   - Yes
   - No
6. If yes to the above question, please explain the type of scam you encountered.
7. What steps do you take to ensure your social media accounts are secure and protected?
8. Are you familiar with the term GDPR? (General Data Protection Regulation)

- Yes
- No

9. How frequently do you review and update your online passwords?
   - Weekly
   - Monthly
   - Every six months
   - Yearly
   - Never
10. Have you noticed personalised content on your social media feeds such as tailored ads or recommendations? How do you feel about this customisation? (Do you believe it is a benefit or a concern for your overall experience?)
11. Are there any specific features or content you would like to see on an online educational platform addressing these topics? (e.g. Infographics, Interactive images, videos, games)
12. Do you prefer learning through written materials such as textbooks or articles or through visual aids such as infographics, images, and videos?
    - Written materials
    - Visual aids

**Adult Survey Questions**

1. Age
2. Gender(optional)
3. Have you ever fallen victim to a phishing scam?
   - Yes
   - No
4. If yes to the above question, please provide details about the type of scam you have encountered.
5. How frequently do you review and update your online passwords?
   - Weekly
   - Monthly
   - Every six months
   - Yearly
   - Never
6. Have you received any formal education teaching you how to protect your privacy online?
   - Yes
   - No
   - Not sure
7. Are you familiar with the term GDPR? (General Data Protection Regulation)
   - Yes
   - No

8. Have you noticed personalised content on your social media feeds such as tailored ads or recommendations? How do you feel about this customisation? (Do you believe it is a benefit or a concern for your overall experience?)
9. Are there any specific features or content you would like to see on an educational platform addressing these topics? (e.g. Infographics, interactive images, videos, games)
10. Do you prefer learning through written materials such as textbooks and articles or through visual aids such as infographics, images and videos?
    - Written materials
    - Visual aids

**Ethics Approval signed form- pdf:**

Alison B ethics.pdf