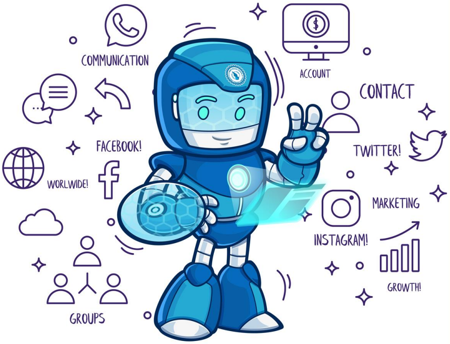


# Cyber Safety Booklet for Children

FOR ADOLESCENTS

Cyber Peace Foundation

Year of Publication: 2019 | Cyber Peace Foundation

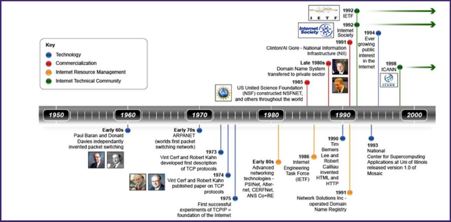
**Content developed and designed by Cyber Peace Foundation**

Ms Neelam Singh | Ms Karuna Bishnoi | Ms Janice Verghese | Ms Akanksha Kapur | Mr Kumar Vikram | Capt Vineet Kumar

**Content Advisory Group**

Shri SN Pradhan, IPS, Director General, NDRF
Shri Rakesh Maheshwari, Group Co-ordinator Cyber Laws and e-Security, MeitY
Dr. Debarati Haldar, Professor of legal studies at Karnavati University
Dr. Manoj, NIMHANS
Dr. Rachna, AIIMS
Dr. Rajesh Sagar, AIIMS
Dr. HK Kaul, DELNET
Ms Jayalakshmi Chittoor, Cyber Peace Foundation

***The idea of a network of computers was thought of in the early 1960s. It was tried in many different ways, and finally ARPANET was created. WIth time, many more changes were made and finally the internet became what we see it as today.***


Key
● Technology
● Commercialization
● Internet Resource Management
● Internet Technical Community
1950
1960
1970
1980
1990
2000
Early 60s Paul Baran and Donald Davies independantly invented packet switching
Early 70s ARPANET (worlds first packet switching network)
1973 Vint Cerf and Robert Kahn developed first description of TCP protocols
1974 Vint Cerf and Robert Kahn published paper on TCP protocols
1975 First successful experiments of TCPIP = foundation of the Internet
Early 80s Advanced networking technologies - PSINet, Alter-net, CERFNet, ANS Co+RE
1985 US United Science Foundation (NSF) constructed NSFNET, and others throughout the world
1986 Internet Engineering Task Force (IETF)
Late 1980s Domain Name System transfered to private sector
1990 Tim Berners Lee and Robert Cailliau invented HTML and HTTP
1991 Clinton/Al Gore - National Information Infrastructure (NII)
1991 Network Solutions Inc - operated Domain Name Registry
1992 IETF
1992 Internet Society
1993 National Center for Supercomputing Applications at Uni of Illinois released version 1.0 of Mosaic
1994 Ever growing public interest in the Internet
1998 ICANN

Source: Presentation by Dr Govind
Former Senior Director, MeitY, and Ex CEO, National Internet Exchange of India
and Advisor Cyber Peace Foundation

# CONTENTS

## CONTENTS

CONTENTS

# PREFACE

This handbook on Cyber Safety is developed with the objective of enhancing the experiences of children and young people with digital devices and technologies. It aims to increase awareness of how they work, the opportunities, potential risks and threats that come with the use of these, and what children can do to use the technology responsibly so as to take maximum advantage of the opportunities and at the same time minimise the risks and potential harm.

It aims to increase awareness amongst the students about digital citizenship, which encourages a positive, smart and responsible approach among the users. By internalizing and practicing the principles of digital citizenship, children can be 'smart and safe' users of technology and become competent to deal with the demands of the increasingly digital world we live in.

While we are looking to equip children for being 'smart and safe' users of technology, we also wish to create an awareness among the teachers, school administration and parents about the opportunities and potential threats in the digital world for children with the aim of creating a favourable and balanced approach in supporting the use of technology by children. There is a need to do everything in our means to develop a safe experience for children and no stone should be left unturned for ensuring this. It is important for all stakeholders to play their part the service providers, parents, schools, government.At the same time it is important that parents and schools avoid being overprotective and inhibit or restrict the use of technology as a way of preventing potential harm.

Giving children the knowledge, skills and capacity to be smart digital citizens and exercise all preventive steps in the use of technology is a much better way of preparing them for confident handling of their adult life as well. The most important aspect is that the Handbook will orient children to the balance they need to maintain in their lives to keep their academic, family and social relationships in balance, to maintain good self-esteem and confidence, They will learn about rationalising the time spent online for various purposes so that they balance online and outdoor activities necessary for their wellbeing and health and also learn how not to abuse their bodies and health through excessive time spent online, while ignoring other activities.

Another major aspect is creating awareness among children about their rights and also their responsibilities in online behaviour.They will learn about digital etiquette and also be made aware about some of their online behaviours which may actually be infringing the law.It is extremely important that children know and understand the boundaries for their behaviours and consequences if these are crossed.

We can do all in our know-how to take preventive steps for protecting ourselves online, however, there will still be a possibility that we come across harmful material or experiences. We need to be confident about sharing and talking about these experiences with trusted adults at home and in school and seeking a solution or redress rather than suffering in silence and feeling isolated. The Handbook also provides information about where to report such incidents, steps to do this and where to seek help.

We aim to undertake this exercise of equipping children with cyber safety skills and good online etiquette and digital citizenship skills in an enjoyable way, through simple reading, 'being smart checklists' and quizzes and competitions.

We hope children and teachers have a wonderful journey together.

# INTRODUCTION

Technological advances are changing the world in ways that could not have been imagined. The emergence of advanced digital innovations are providing new opportunities to connect and learn, and have begun influencing every aspect of human life.

Children and young people have shown greater ability to adapt and adopt digital devices and innovations, which augurs well for the future. They use the devices and apps for a variety of functions, including self-expression, communication, networking, research, entertainment, and much more. The internet has enabled children to become active social agents and to mobilise for social, ecological and other causes. They are increasingly able to project their voices with unprecedented reach.

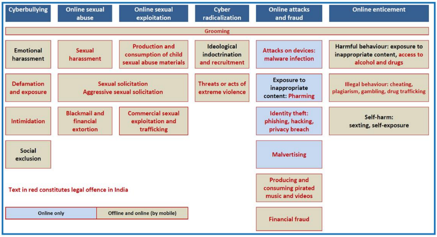
However, an assumption is often made that young people have superior skills with digital technology, which surpass those of their parents and teachers. It may or may not be right. Many young people are confident in using a wide range of technologies and often turn to the internet for information. They seem able to learn to operate unfamiliar hardware or software very quickly and may take on the role of teaching adults how to use computers and the internet. But the confidence with digital technology can also be misleading.

Many of them frequently struggle when applying them to research tasks. They can find it difficult to work out whether information on an unfamiliar website is trustworthy, and rely on their chosen search engine's rankings for their selection of material. They may not understand how search terms work or of the powerful commercial forces that can result in a particular company being top of the search engine's list. They may not be aware of the lurking risks and threats and the fact that some of their actions can invite them trouble.

Furthermore, the digital skills and knowledge are not evenly spread amongst all young people. Dearth of research on the subject has prevented a nuanced analysis of who are most likely to lag behind in the opportunities afforded by technological advances. However, there is general agreement among those working on cyber safety and security among children and young people that gender is a major impediment. Social norms have impeded girls' access to opportunities, including the access and use of digital devices and the internet. Many of them belonging to socially or economically marginalised families in rural, semi-urban and urban areas have either no access, or limited, or supervised access to digital technologies, which could enable them to exercise their agency, autonomy and rights in an increasingly interconnected world.

The exploration of new vistas and acquisition of rich experiences online require a strong element of caution. After all, every light has its shadow. The technologies can be misused or overused in ways that are detrimental to the users and even non-users.

UNICEF in its Child Online Protection in India report in 2016 had presented the following typology of risks and threats



| Cyberbullying | Online sexual abuse | Online sexual exploitation | Cyber radicalization | Online attacks and fraud | Online enticement |
|---|---|---|---|---|---|
| Grooming | | | | | |
| Emotional harassment | Sexual harassment | Production and consumption of child sexual abuse materials | Ideological indoctrination and recruitment | Attacks on devices: malware infection | Harmful behaviour: exposure to inappropriate content, access to alcohol and drugs |
| Defamation and exposure | Sexual solicitation Aggressive sexual solicitation | | Threats or acts of extreme violence | Exposure to inappropriate content: Pharming | Illegal behaviour: cheating, plagiarism, gambling, drug trafficking |
| Intimidation | Blackmail and financial extortion | Commercial sexual exploitation and trafficking | | Identity theft: phishing, hacking, privacy breach | Self-harm: sexting, self-exposure |
| Social exclusion | | | | Malvertising | |
| | | | | Producing and consuming pirated music and videos | |
| | | | | Financial fraud | |

Text in red constitutes legal offence in India

| Online only | Offline and online (by mobile) |
|---|---|

**_Source: UNICEF India Report_**

The above classification presents a birds' eye view of the risks and threats which contribute to the vulnerability of children and young people in the digital age. The other side of the coin is resilience among them, which needs to be nurtured and strengthened in order to empower them for the challenges and opportunities introduced by digital technologies.

The optimal safeguard for children is to facilitate their access to the internet, protect their privacy, encourage self-expression, and ensure that they can recognise potential dangers and know what to do about them. The concept of digital citizenship has emerged as a useful framework of various facets that need to be developed and strengthened.

## Basically, there are nine elements of digital citizenship.

***1. Digital Access:*** Equitable distribution of technology and online resources is an important issue from the perspective of human rights and social justice. In view of the proliferation of digital technologies and access to several essential services depending on digital access, all efforts should be made to bring those without access under the digital umbrella and empower them with digital literacy.

***2. Digital Literacy:*** Understanding technology and its use is the basic condition for optimising its benefits. Going beyond reading and writing, digital literacy encompasses the understanding of how digital media operates, how good information and real news can be discerned from the unlimited reservoir of information and "fake news" respectively, and the ways in which online communication can be effective.

***3. Digital Communication:*** The electronic exchange of information with other people, through emails, cell-phones and instant messaging, constantly and without delay, requires appropriate decisions by users who are faced with several options. Basic communication principles in tandem with the ever-expanding features of digital devices and technologies highlight the factors that should determine the decisions of the users.

***4. Digital Commerce:*** Increasing buying and selling of goods and services has opened vistas for the sellers, service providers, and consumers. But they must have the tools and safeguards in place to assist with buying, selling, banking, or using money in any way in the digital space. Such knowledge is particularly important for students who wish to employ the tools of technology in exploring and determining the path to their future.

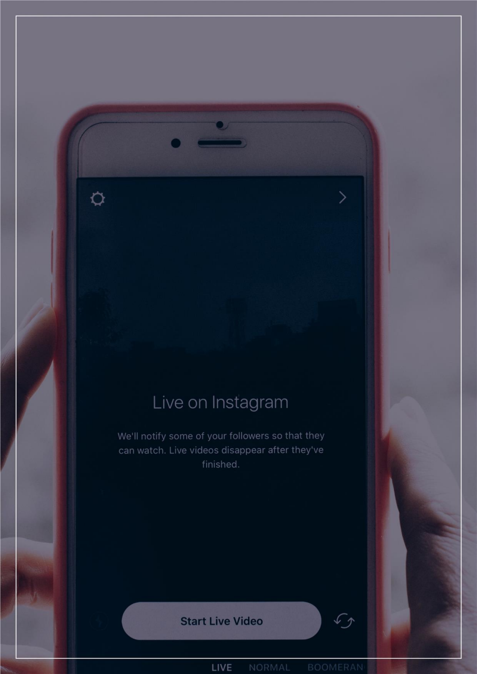
***5. Digital Etiquette:*** Digital etiquette describes the norms or appropriate and responsible behaviours while using technology devices. One needs to be aware of and practice appropriate and ethical behaviour in a variety of digital environments. This includes shaping your digital reputation and being a responsible citizen of the communities in which you participate, from school groups, to games, to social networks.

***6. Digital Health and Wellness:*** A collective sense of rights and responsibilities is important in a digital society for maintaining social harmony and increasing productivity. Basic digital rights must be addressed, discussed, and understood and users must help define how the technology is to be used in an appropriate manner.

***7. Digital Rights, Freedoms and Responsibilities:*** A collective sense of rights and responsibilities is important in a digital society for maintaining social harmony and increasing productivity. Basic digital rights must be addressed, discussed, and understood and users must help define how the technology is to be used in an appropriate manner.

***8. Digital Security:*** Awareness of potential online risks, threats and attacks and the ways and means of preventing them are important skills to have in an interconnected world. While cautious conduct can ward off attempts at invasion of privacy and manipulation, electronic precautions can secure digital devices and usage. Viruses, worms and other bots can be passed along from one system to another wherever the devices are being used.

***9. Digital Law:*** At the core of digital citizenship are basic ethics, which are reflected in national and international laws. They prohibit certain actions unanimously and categorically while developing understanding and consensus on the ways of addressing new challenges posed by digital technologies. The users are morally and legally duty bound to exercise caution based on the existing laws and rules that regulate processes influenced by digital technologies and provide protection from criminal activities and civil misdemeanors.


Live on Instagram
We'll notify some of your followers so that they can watch. Live videos disappear after they've finished.
Start Live Video
LIVE
NORMAL
BOOMERAN

# 1. Digital Access

### *1.1 What is digital access?*

"People who have access to digital technologies stand to gain in an interconnected world. All they need is a connection to the internet and devices such as smartphones, desktop or laptop computers, or tablets, to send and receive written, audio and visual messages without delay, perform endless number of tasks, access essential services and information on a wide variety of topics. Those who do not at a high risk of missing out on these and many other opportunities".

With various telecom companies competing against each other to capture the huge Indian market by offering better and cheaper plans, India probably has the world's cheapest mobile data packs. A study of data from 6313 mobile data plans across 230 countries over a period of around one month, October 23 to November 28, 2018, found that Indians pay an average of Rs 18 for one gigabyte of data as against the global average of Rs 600. The researchers studied 57 plans in India and concluded that the cost of 1 GB of data for the Indian user ranged between Rs 1.41 and Rs 98.33.[1]

The internet usage in India had exceeded half a billion people - 566 million as of December 2018.[2] Of the total user base, 87 percent or 493 million Indians were defined as regular users as they had accessed internet in last 30 days. Nearly 293 million active internet users reside in urban India, while there are 200 million active users in rural India. The report found that 97 percent of users use mobile phone as one of the devices to access the internet.

Improved infrastructure and connectivity is expected to improve digital access in rural areas, even the most far flung. Indeed, rural areas are fast catching up with urban areas in terms of digital access. But efforts still need to be made to ensure that no one is denied digital access.

### *1.2 Newer vistas with digital devices and Internet*

Technological innovations can be seen everywhere, in our homes, classrooms and in our surroundings too.
Can you name 5 things that use modern technology around you?

The following categories of devices perform different but interlinked functions.

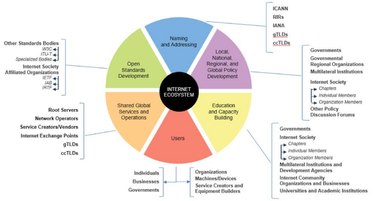
a) Mobile phones, desktop and laptop computers, tablets
b) E-readers, e.g., Kindle
c) Dongle and Wi-Fi router
d) Internet connected printer
e) Internet Of Things (IoT) Devices: Smartwatches, Smart TV, Smart refrigerators, home assistants (e.g., Alexa, Google Home, and Siri)
f) Whiteboards and smart boards in smart classrooms.

These innovations have made lives easier than ever before but their misuse and exploitation can aggravate unanticipated risks.

[1] *https://trak.in/tags/business/2019/03/07/indias-internet-packs-are-the-cheapest-in-the-world-is-jio-the-reason/*

[2] Kantar IMRB. ICUBE 2018

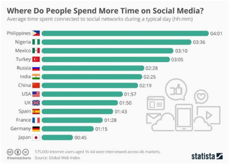
## Internet Ecosystem Stakeholders


INTERNET ECOSYSTEM
Naming and Addressing
Local, National, Regional, and Global Policy Development
Education and Capacity Building
Users
Shared Global Services and Operations
Open Standards Development
ICANN
RIRs
IANA
gTLDs
ccTLDs
Governments
Governmental Regional Organizations
Multilateral Institutions
Internet Society
Chapters
Individual Members
Organization Members
Other Policy Discussion Forums
Governments
Internet Society
Chapters
Individual Members
Organization Members
Multilateral Institutions and Development Agencies
Internet Community Organizations and Businesses
Universities and Academic Institutions
Organizations
Machines/Devices
Service Creators and Equipment Builders
Individuals
Businesses
Governments
Root Servers
Network Operators
Service Creators/Vendors
Internet Exchange Points
gTLDs
ccTLDs
Other Standards Bodies
W3C
ITU-T
Specialized Bodies
Internet Society Affiliated Organizations
IETF
IAB
IRTF

Source: Presentation by Dr Govind
Former Senior Director, MeitY, and Ex CEO, National Internet Exchange of India
and Advisor Cyber Peace Foundation

The Internet is an interconnection of networks that uses internet protocol to link devices worldwide. With digital devices and access to the internet, several functions can be performed quickly and simultaneously. For instance: sending and receiving email, using social media, watching movies and television series, accessing large open information library from millions of websites, and writing blogs.

Digital technology is primarily used these days with new physical communications media, such as satellite and fibre optic transmission. A modem is used to convert the digital information in the computer, mobile phone, and other such devices to analog signals for the phone line and to convert analog phone signals to digital information for the computer.[3]



*https://www.statista.com/chart/18983/-time-spent-on-social-media/*

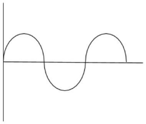
According to an estimate, an Indian on an average spends two hours and 25 minutes on social media.

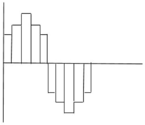
3 *https://whatis.techtarget.com/definition/digital*

### *1.3 Bits and Bytes*

Radios and telephones conventionally used analog technology for electronic transmission. The data was conveyed through electrical signals of varying frequency or amplitude, which were added to carrier waves of a given frequency.

Scientific progress has enabled the electronic technology to generate, store and process data in various forms. The number 1 denotes the positive while 0 represents the negative. Data is stored or transmitted with digital technology in strings of 0 and 1. Each of these state digits is referred to as a bit (and a string of bits that a computer can address individually as a group is a byte).


**Analog Signal**


**Digital Signal**

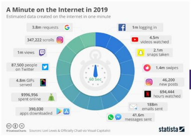
### *1.4 Navigating the Cyberspace*

#### 1.4.1 Internet and the World Wide Web

Internet may be considered a vast network of networks, which enables access to any and every kind of information. The following graphic developed by Statista gives an idea of the humongous amount of activity that takes place on the internet.

"The World Wide Web, commonly known as www, is one of the networks which is used by most of the legitimate users to navigate using search engines like Google, Yahoo, Bing and DuckDuckGo. But it is just the tip of the iceberg. Beyond it and unreached by the regular search engines is the Deep Web.

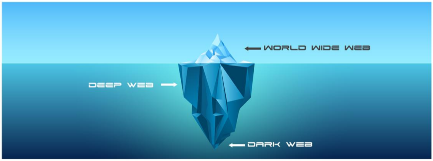
Indeed, the vast Internet consists of three layers. The first layer is public, consisting of sites we use frequently such as Facebook, Twitter, Amazon and LinkedIn. This layer makes up just about 4 to 6 percent of the entire Internet. The remaining 94 to 96 percent is the Deep Web and the Dark Net. "



Source:
https://www.statista.com/chart/17518/internet-use-one-minute/

### 1.4.2 The no go zone: Deepweb and Darknet

The Dark Net, or hidden web, is the space for most of the serious online offences against children. The Dark Net, is recognized as the underworld or the "Wild West" of cyberspace and cannot be accessed using Google or other regular search engines.



The Deep Web, the second layer, is a network where data is stored in inaccessible databases. It includes all web pages, websites, intranets, networks and online communities that are intentionally and/or unintentionally hidden, invisible or unreachable to search engine crawlers. It is also known as the hidden web, undernet, Deep Net or invisible web.

The Dark Net, or hidden web, is the third and deeper layer of the Internet is recognized as the underworld or the "Wild West" of cyberspace. It is a network of networks that are not indexed by search engines such as Google, Yahoo or Bing. These are encrypted networks that are only available to a select group of people and not to the general internet users, and only accessible via authorization, specific software and configurations. This includes harmless places such as academic databases and corporate sites, as well as those with shadier subjects such as black markets, fetish communities, and hacking and piracy.

As it provides anonymity to the users, this is where hackers congregate and facilitate illegal meetings. The type of site most commonly associated with the dark web are marketplaces where illicit goods such as narcotics, firearms, and stolen credit card numbers are bought and sold. The darkest corners are used to hire hitmen, engage in human trafficking, and exchange child pornography. More than that, though, the dark web contains content and data that can be accessed with anonymity. It could be a blog, forum, chat room, or private gaming server. Customers whose data is breached do not have access to the darknet.

### 1.4.3 Administration of the cyberspace

As the internet and world wide web does not respect territorial boundaries, the role of the national laws and mechanisms is limited in the management of the cyberspace. The national governments do invest in the infrastructure and development of technical and human resources, the legal regime remains compromised. The servers of most of the internet service providers are situated in the United States and Western Europe, and are beyond the jurisdiction of Indian or any other national law. The internet service providers insist on removing or blocking access to only that content which violates their community guidelines.

International law provides for some mechanisms for negotiations on varied aspects of cyberspace management and security but there are, as of now, plenty of hindrances. As the global consensus on unacceptability of child sexual abuse materials (including images) on the internet has brought the governments and industry on the same page, the action to take them down tends to be prompt. International inter-agency cooperation against cybercrimes is ongoing but the common cause has to be agreed upon in many other areas.

In principle, digital technologies expand the horizons of the users by allowing them to look beyond national and geographical boundaries. Well almost. Governments can block the services of internet service providers. They may even insist on local versions, which permit them to negotiate restrictions with the internet service providers on access to any content deemed illegal or offensive in their country.

**Box: Restrictions on internet in some countries**

Pakistan had banned YouTube for about three years following violent protests across major cities against the uploading of an anti-Islam film on the site in September 2012. It permitted a new version of YouTube, which allowed the Pakistan Telecommunication Authority (PTA) to seek access to offending material to be blocked within the country.

China has blocked Google, Facebook, Twitter and Instagram, as well as thousands of other foreign websites, including The New York Times and Chinese Wikipedia, over the past decade. Nonetheless, it has not disrupted the access of Chinese people to internet. A range of Chinese websites such as Baidu, WeChat/Weixin, Sogou, So 360) perform the same functions even though with a strong dose of censorship.

Based on media reports[4]

Consider some of its implications. The internet industry has the ambitious task of administering the cyberspace and ensuring its safety. Technological advances are making that happen but it is a moot question if they can keep pace with the mischief that is being played.

## 1.5 Barriers to digital access

The ability to afford digital devices and internet was for long associated with digital access. The devices have become cheaper over the years with easy availability of a wide variety of

[4] https://www.reuters.com/article/us-pakistan-youtube/pakistan-lifts-ban-on-youtube-after-launch-of-local-version-idUSKCN0UW1ER

https://www.independent.co.uk/life-style/gadgets-and-tech/features/china-internet-social-media-great-firewall-of-china-censorship-apps-a8510036.html expensive and inexpensive smartphones. The competition between internet service providers has proved to be a boon for the consumers who can choose from a range of affordable internet packages or plans.

Some attributes characterise the people who are more likely to have digital access. These include: working knowledge of English as most of the online/digital applications are in English, the ability to use computers and computer related technologies, an aptitude for efficient use of technology, easy access to digital devices and the internet, and the ownership of the internet connected digital devices. As a result, they are likely to receive information quickly and save their time with functions such as accessing financial services, public services, information and knowledge, and a host of other services than those who are not good at using technology.

It needs to be noted that the diffusion of technology is no longer impeded by financial resources. An expensive smartphone as well as an inexpensive simple one can perform similar functions. Indeed, the consumers may be categorised into the "haves" who make good use of basic functional devices, the "have lots" who possess more expensive, sophisticated and good-looking devices and usually perform similar functions, and the "have-nots" who either lack access or are allowed usage under strict supervision.

The "have nots" in the digital era are usually the first-time users with low confidence in technology as well as their own abilities to master it are deprived of many opportunities. Thus, the technologies need to be demystified and they need to be encouraged to use the technologies for their own benefit.

Furthermore, that urban people use information more frequently than the rural one may no longer be true. The digital divide between rural and urban communities is narrowing down with the rapid diffusion of technologies. The issues of connectivity are being sorted out.

However, socio-cultural barriers have restricted the access of some important groups in society to digital technologies. Often either due to biased perception of the lack of need by women or because of notions of safety for girls, their access to technology is restricted. These barriers need to be removed so that equal opportunities are available to all for benefiting from digital access. The interface of children and young people with disabilities with digital devices has also not been tested, explored and promoted whereas they may gain immensely from the technological advances.

# 2. Digital Literacy and Fluency

### *2.1 What is digital literacy?*

Digital literacy is, in addition to reading and writing, the ability to use digital technology, communication tools or networks to locate, evaluate, use and create information. It involves reading on digital devices, gauging the credibility of a website, creating, packaging and sharing information in ever-increasing ways and learn social responsibility while interacting on social media.

### *2.2 Eight components of digital literacy* [5]

#### *2.2.1 Functional skills*

Proficiency in reading, writing and arithmetic was for long been regarded as the basic minimum for getting on in life. These three R's are still relevant but they need to be supplemented with additional knowledge and skills that allow you to use digital devices and navigate the cyberspace. The ability to complete basic internet searches, work on spreadsheets and PowerPoint presentations provide you with the opportunity to use a wide range of technologies collaboratively, creatively and critically. These abilities facilitate learning and provide new avenues for professional advancement.

The new age functional skills have also become essential in daily lives for a variety of reasons. Online banking transactions are quicker and more efficient. The Aadhar card is required to access many basic services. Several tax returns have to be filed online. For example, income tax, general sales tax. As the government's thrust is on "Digital India", digital connectivity and communication will become increasingly important.

#### *2.2.2 Creativity*

Digital technologies facilitate self-expression, creativity and learning by enabling the users to do innumerable things with high level of finesse and accomplishment. For instance, creating, packaging and sharing information, creative writing or academic research. analyses of data, taking pictures, making videos and multimedia products. The drudgery is reduced. Presentation skills improve with the availability of a large variety of options. Sharing is easier and inexpensive. And considerable reduction in the use of paper has some environmental benefits.

#### *2.2.3 Critical thinking and evaluation*

Critical thinking is the process of evaluating information, questioning it, and determining if it's worthwhile. Everyone should know how to think critically.

a) You can practice critical thinking by asking these basic questions:
b) Does someone or an organization benefit from this information?
c) Does this information sound biased toward one side or another?
d) Can you tell the author has an opinion?
e) Does the heading or headline match the information in the body?
f) Does the information conflict with something you know to be true?

Critical thinking will lead you to ask questions and find answers. You could explore information that you wish to know more about. You could investigate any information that you doubt. The earlier you learn to think critically, you would be better equipped to learn, verify facts and spot misinformation or "fake news".

It is also important to pause and reflect while online. Digital technologies allow us to undertake several functions simultaneously, which increases the chances of careless decisions and wrong clicks. The result could be miscommunication or exposure to threats and risks.

[5] *This classification is drawn from the following:*

*https://www.researchgate.net/figure/Components-of-Dig ital-Literacy-The-eight-components-include-creativity-critical_fig1_328513105*

*http://www.curriculum.edu.au/leader/digital_literacy_across_the_curriculum,33211.html*

### *2.2.4 Cultural and social understanding*

Children and young people are actively using digital media to participate in social and cultural life outside school. Making and sharing media has become an important part of how children communicate with each other these days. Children have to know how to negotiate information in text, visual, audio and so on and how to represent meaning effectively and creatively through these media. Children create and edit their own cartoons, videos, animations, music or other media and share these with friends. Many children may be sharing videos, YouTube, jokes, photos etc with their friends with the aim of having fun or communicating with them. Digital literacy will help to expand and extend your creative use of technology actively in your social and cultural interactions.

### *2.2.5 Collaboration*

Collaboration is working among and across personal and global networks to achieve common goals. The interconnectedness in the digital world, which is now taken for granted, is an outcome of the collaborative efforts of several individuals, teams, agencies, institutions and governments. Due to the interconnected world, the effects of what is happening in one place can have repercussions in other places, what is affecting a few can affect very many. Real-time transmission of information and weakening of geographical boundaries due to the digital revolution have their pros and cons, which may be discussed ad infinitum.

The following are some of the implications, which can be harnessed and put to good use.

**a) New ways of working.** Digital technologies enable non-hierarchical leadership based on individual skill sets. When many individuals connect, interact and contribute, solutions to even the most complex problems and processes can be dealt with.

**b) Efficiency and effectiveness.** The group interactions can be productive when certain rules of engagement are agreed upon, personal and civic responsibility is assumed on the basis of competency, and disagreement is acknowledged, respected and addressed with open and flexible approaches.

A peculiar challenge emanating from cross border digital infrastructure is the issue of jurisdiction. There are tricky situations in which the victim is in one country, the offender in another country, the server in a third country. The trail may be established but dealing with national laws of various countries requires transnational collaboration and calibration among national governments and the internet industry.

The national laws can be invoked or applied within national boundaries. How can problems be addressed when the trail covers a number of countries, and at times, international waters? As of now, international treaties which national governments sign up to in order to address cross-national issues do not provide easy solutions to this problem.

### *2.2.6 Ability to find and select information*

Online browsing has made research much easier but in many ways more challenging. Now one has easier access to virtually endless information. The challenge is to check the veracity of the sources as well as the information.

The following are a few pointers for checking the veracity of the source of information.

***a) Is the author listed on the information/news?*** If yes, they are claiming personal responsibility for the information that is being conveyed. If the information is inaccurate, their reputation and probably career could suffer. Has the author mentioned the resources used?if yes this can help verify the information.

***b) A date shows if the information is current.*** Information changes very fast, thanks to the Internet and to verify if it is still valid, a date is necessary. The information may not probably is no longer relevant. If there is no date at all, it may not be credible.

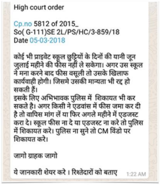
***c) Is the domain credible?*** The domain names say a lot about websites, .com, .edu, and .gov are among the most credible domain endings for websites. Other variations are much less credible. So check the URL name. If any of those three options end a URL, it indicates the website's credibility.

***d) Is the website designed properly?*** Web design is surprisingly important in verifying a website's credibility. If someone didn't put work into their website to make it look good, you can't trust that they've put the necessary effort into verifying their information.

***e) Are the spelling and grammar in the writing correct?*** The logic is simple - it reflects how seriously the production and dissemination of information is taken. If there was no attempt to check the grammar and spelling, probably the accuracy of the information was not checked carefully.

***f) Credibility of information.*** Everything on the internet or on a social network should not be taken at face value. A lot of motivated or misleading information and fake news is circulated through networks. An unbiased judgement based on critical thinking can help to determine if the information is trustworthy. The recipient of information needs to decide on the veracity of the message, if need be cross-checking it from multiple sources.

The following message was circulated through WhatsApp in India in 2018. It seemed credible due to its style of presentation and language. But careful scrutiny and investigations revealed that it was false and used the reference tag of an order issued by the High Court of Sindh in Karachi, Pakistan, in 2015.



High court order

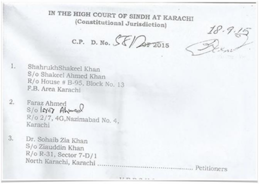
Cp.no 5812 of 2015_
So( G-111)SE 2L/PS/HC/3-859/18
Date 05-03-2018

कोई भी प्राइवेट स्कूल छुट्टियों के दिनों की यानी जून जुलाई महीने की फीस नहीं ले सकेगा। अगर उस स्कूल ने मना करने बाद फीस वसूली तो उसके खिलाफ कार्यवाही होगी। जिसमे उसकी मान्यता भी रद्द हो सकती हैं।
इसके लिए अभिभावक पुलिस में शिकायत भी कर सकते है। अगर किसी ने एडवांस में फीस जमा कर दी है तो वापिस मांग लें या फिर अगले महीने में एडजस्ट करा दे। स्कूल फीस ना दे या एडजस्ट ना करे तो पुलिस में शिकायत करे। पुलिस ना सुने तो CM विंडो पर शिकायत करे।

जागो ग्राहक जागो

ये जानकारी शेयर करे । रिश्तेदारों को बताए 1:22 AM

***Message Forwarded on WhatsApp in Delhi, India***



IN THE HIGH COURT OF SINDH AT KARACHI
(Constitutional Jurisdiction)

18.9.15

C.P. D. No. 5812 ~~of~~ 2015

[illegible]

1. ShahrukhShakeel Khan
S/o Shakeel Ahmed Khan
R/o House # B-95, Block No. 13
F.B. Area Karachi

2. Faraz Ahmed
S/o Israr Ahmed
R/o 2/7, 4G,Nazimabad No. 4,
Karachi

3. Dr. Sohaib Zia Khan
S/o Ziauddin Khan
R/o R-31, Sector 7-D/1
North Karachi, Karachi ........................................ Petitioners

***Actual Order at Karachi, Pakistan***

**Box: Online resources for digital education**

Countless resources on the Internet provide information about digital technologies. Some are free while others seek payment for access to the full range of information materials. For example:

E-Pathshala, initiated by the Ministry of Human Resource Development (MHRD) and the National Council of Educational Research and Training (NCERT), hosts resources for teachers, students, parents, researchers and educators that is available on the Web, Android, IOS and Windows platforms. A wide variety of print and non-print materials, including textbooks, audio, video and periodicals can be accessed online or downloaded for offline use at ***http://epathshala.ncert.org.in/epathshala.php?id=Students&type=&ln=en.***

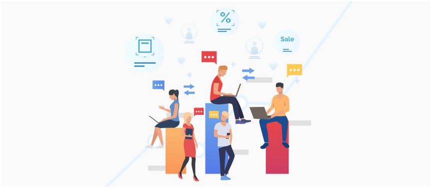
Khan Academy makes available a range of online tools and short video lessons on its YouTube™ channel and website www.khanacademy.org, which students can use to understand various lessons and concepts easily.

Various open source resources, video lectures on YouTube™, skillshare and GitHub are available to enhance technological skills, including software development and coding. Your teachers can recommend other useful websites and portals. And you can also do your own online research.

### *2.2.7 Effective communication*

**Real-time communication**

Digital technologies now facilitate immediate communication which may be one to one, one to many, or among many. This can be through voice calls, video calls, instant messaging platforms, SMSes , etc.



**Offline and online transition.** When connected with the internet, you can read online with the aid of a web browser. You can also download the content for offline reading when you are connected and viewing later on even without the internet. Some devices, like Kindle, facilitate offline reading. There are advantages and disadvantages of both. When reading online, the resource will open quickly, but the pages open one at a time, so there may be some brief load times when flipping pages. Offline, the resources may take several seconds to open as the entire file is decrypted. However, once that process is complete, pages open rapidly.

### *2.2.8 E-safety*

When connected with the internet, you can read online with the aid of a web browser. You can also download the content for offline reading when you are connected and viewing later on even without the internet. Some devices, like Kindle, facilitate offline reading. There are advantages and disadvantages of both. When reading online, the resource will open quickly, but the pages open one at a time, so there may be some brief load times when flipping pages. Offline, the resources may take several seconds to open as the entire file is decrypted. However, once that process is complete, pages open rapidly.

***Points to remember:***
Have your digital devices been installed with antivirus software?
When did you last update the antivirus software on your digital devices?

***The classification is drawn from the following:***

*https://www.researchgate.net/figure/Components-of-Digital-Literacy-The-eight-components-include-creativity-critical_fig1_328513105*

*http://www.curriculum.edu.au/leader/digital_literacy_across_the_curriculum,33211.html*

### 3.1 *What is digital communication?*

If digital literacy is about the ability to read, understand and interpret digital processes, digital communication is the ability to employ these processes to connect and interact with others.

Digital communication or communicating with others through digital media can stimulate social relationships. The users can stay in touch with friends, revive and enrich their existing relationships and create new ones. Many people who have less or not so good social relations may use it to compensate for this and build new and positive relationships. Enabling students to communicate and collaborate in the digital world helps enhance their learning process.

***Box 3.1: Circuitry of digital communication***

Source: Cyber Peace Foundation

In plain and simple one-way communication, there is a sender who sends a message through a medium to a receiver. Verbal communication involves someone speaking and someone listening. Interpersonal communication occurs when the sender and receiver exchange their roles, and speak and listen to each other through a process that facilitates understanding, agreement or disagreement. Visual communication involves someone showing a visual product (e.g., a picture, video, animation) and someone watching.

Interpersonal verbal communication and written communication from real life is changing to digital communication in a virtual life. The interface between humans and technology allows one or many senders whose messages can get aggregated. For instance, the email can be copied to many people. The discussion on social media allows aggregation of messages. As discussed earlier, the medium is more complex. The receivers can be one or many.

Children need to develop competency in operating in both lives and maintain functional independence for this. The two worlds do overlap and at the same time provide contrasting experiences. A balance has to be maintained.

**Real versus virtual lives**

| Real lives | Online lives |
|---|---|
| Offline activities | Online activities |
| Direct socialising | Social networking |
| Face to face communication | Text messaging |
| In person interactions | Internet connections |
| Live in local community | Live in worldwide web |
| Exist more privately | Exist more publically |
| More engagement demands | More escape opportunities |
| Limited information | Unlimited information |
| Careful communication | Less inhibited communication |
| Have to take responsibility for personal actions | Potential anonymity makes evasion of responsibility possible |
| History remembered | History recorded (footprints left) |
| Parents feel more in control | Parents feel less in control |

Parents in some cases may have grown up only in the real world, so for them it will take effort to understand the changing scenario arising with the technological realities of the current times. Virtual media can replace real life: Parents need to establish boundaries that prevent virtual media from pushing out real, flesh-and-blood relationships and activities. Parents need to inform teenagers about risks to watch out for and rules to follow and self-management responsibilities to be learnt in order to maintain their online freedom and maintain a healthy balance between offline and online activities.

### *3.2 Opportunities and risks*

One has to use the internet smartly and responsibly while being conscious of the opportunities, potential threats and disruptions.

Online activities provide an opportunity for adolescents to test their opinions and attitudes, experiment with identity, experiment with social relationships and in the perception of anonymity also take risks which they may not in real life. Adolescents sometimes show weak control over time spent online, over their own activity timelines, and priority setting. Online games can be addictive, balancing with outdoor activities is essential.

Children also need to develop critical thinking with regards to content consumption. Also the need to take care that online relationships, providing an escape from the sometimes difficult relationship challenges, do not become a substitute for real life relationships. Teens growing up in a virtual world confront daily choices that will shape their character and influence their capacity for life and their future as well. Online games and social media technologies can create an artificial existence which will disrupt normal life and therefore balance and moderation is essential and critical thinking about their own online activities.

There has been a shift from interpersonal to digital communication after the rise of the Internet. This has contributed to a general loss of the personal connection and development of face-to-face interactions. We can now talk and text even when away from each other. It has even changed the way we communicate when near each other, as many people will text a friend or loved one who is in the same room in order to keep a conversation or comment secret.

Technology has limited students' ability to communicate effectively in face-to-face contexts with a range of diverse people. With social media, students are able to expose themselves to a limited cross-section of people — typically others who are similar and have comparable values, beliefs and attitudes. As a result, it has impaired their ability to communicate with others who are different from them. Though new communication opportunities have increased the ability to connect with people across the world quickly and effectively, the quality of these relationships has taken a hit. Communicating face-to-face is still a very important component of building a lasting rapport with someone which is an essential skill in daily life in a community or at work and everyone has to make an effort to keep these skills intact.

Everyone needs to be conscious of this and use technology in a way that it does not become a substitute for real life communication but remains a smart additional channel which is not allowed to compromise basic good interpersonal communication skills essential for success in all aspects of our life.

Remaining connected with friends, family and acquaintances is an attractive idea. But it can create certain situations that can be awkward and difficult to deal with.

In-the-moment communication through instant messaging, texting, and posting comments online is common. It does not allow enough time to reflect, react and respond on the basis of informed understanding of conversations that are getting rude or mean. But learning to exit such conversations is essential. You may have to sign off instant messaging, not respond to a rude text, or stop yourself from posting a comment on Facebook or Instagram.

***Forwarding information***

Responsible sharing

***One has to think and take responsibility for the communication one posts online.***

***Forward information or posts received after you verify the source and the contents of the post. It is not good to share false information.***

***Stop yourself from sharing posts that are offensive or obscene. Be respectful and empathetic towards others***

***Personal information that you share can be used against you. Review the content that you wish to share online and only provide information that is essential and absolutely necessary.***

***Use trusted sources for downloading online. Downloading songs and movies from untrusted sources may be illegal and you should not be sharing these with your friends. Use trusted websites or platforms, like Google Play Store, Apple App Store, Gaana.com, Saavn, Netflix, etc.***

***Personal responsibility for information posted online and sent via text***

***Posting photographs***

Often family, friends, acquaintances and strangers post photographs on social networking sites. Usually they do not seek consent of the person whose photograph they post. While their intention may not be bad, the photograph can be misused by a wide variety of other people. It is a good idea to convey your concerns if you do not want your photographs posted.

***Sharenting and its risks***

Many parents overshare pictures of their children online and in the process undermine their right to privacy, cause embarrassment, hurt and bullying, and damage online reputation.

Sharenting reveals aspects of children's life on social media without their consent. They may be too young to fully understand but it is important to consider the consequences from their perspective. Posting of a picture of a child with a funny caption, relating to their hair or facial expression, could upset them when they are older or make them a butt of bullying by others. Every post contributes to a record of photos, shared links and comments. This record is hard to delete and can shape the child's online reputation.

***"Stranger danger"***

As in real life, there are strangers, acquaintances and friends online. How one communicates, how much and what kind of information is shared depends on the equation and level of trust people have in one another.

It is important to choose online friends wisely. Be wary of new online friends. Do not trust them easily because who knows who they are. There are many cases of people faking identities with not so good intentions. They may be people known to you, who wish to dig out more information out of you. They may be strangers, who wish to gain and then betray your trust.

***"Grooming"***

Sometimes strangers, or even people who are known, build an emotional connection with children and young people online or face-to-face to gain their trust for the purposes of sexual abuse or exploitation. Many children and young people begin to feel that a special friendship or relationship is developing and do not understand that they are being groomed. "Grooming" is subtle but has serious consequences.

***Recognize ways that people online may seek to persuade you.***

**a) Bribing:** This can range from offering money and gifts. The gifts may even be in the form of points or lives and in-game rewards in an online game.

**b) Flattery:** Constant attention and praise can be a way of winning the affection of the targeted child.

**c) Sexualized games and intimacy building:** Gradual introduction of subtly sexual allusions in conversation or during play are used to test the child's vulnerability. If the child positively responds to his overtures, he will attempt to build further intimacy with the child.

**d) Desensitization:** They try to desensitize the child to sexual acts by showing the child, pornography and child sexual abuse imagery. Constant exposure to explicit content may 'normalize' sexual behavior for the child and 'desensitize' her/him.

**e) Threats and blackmail:** They employ forceful coercion to gain access to the child.

**f) Scattergun approach:** When they do not know what the child will respond to, they may try all of the above in an effort to win the child's attention and interest.

Inform and discuss with friends, family members, teachers or anyone you trust any annoying or uncomfortable occurrence or activity such as extra friendly behaviour, cyber stalking, bullying and strange behavior online.

***Viewing inappropriate content***

As you access the internet independently and increasingly, you may come across content which is not suitable for your age or development stage. This may include information or images that are adult in nature, may be sexually explicit, very violent and can upset you or influence you to unlawful behaviours. Accessing inappropriate content is possible through any internet enabled device and can happen accidentally even when you are not actively searching for it through websites, gaming apps, links sent to you or while chatting with your friends. You may not be developmentally ready to deal with what you see by yourself so share your experience and concerns with your parents or a trusted adult.

One way of avoiding inappropriate content unsuitable for your age group is to always stick to games and apps indicated for your own age group. Prevention is one thing but this does not always ensure that you will not see anything inappropriate for your age at all. If this happens or you are upset, confused or worried about anything you have come across through the internet, you should talk to your parents or a trusted adult.

***Gaming:*** Games can offer young people a sense of escape from the reality of the world and the social aspect of some games can help children feel part of a community. More and more children and young people are joining the online gaming community. Easy access and a range of platforms that can be used for playing online games are increasing online gaming in India.

Children play online games on mobiles, consoles, computers, portable gaming devices and social networks. The gaming consoles operate like a computer where you need to create your account, login, put a headset, use a webcam or other devices. You not only play games with several users online but also talk to them, share your views, become friends, join groups, teams, etc.

Wherever there are a lot of users on internet, cybercriminals find their way to victimize them.This can be in way of cheating, cyber bullying, sharing inappropriate content, etc. and sometimes gaming addiction. While online games can be a fun way to connect with people, they also bring associated risks and it is important for you to understand the potential risks and know how to handle certain situations. Have fun but be safe!

***Potential risks associated with online gaming***

a) Some games let children play and chat with anyone in the world. There are many aggressive players online who may bully you. Some players play simply to bully or harass others. They may use inappropriate language or cheat others. It is important for you to be careful.

b) Some young people through online games are abusing the fear around the challenge to encourage others to self-harm and carry out various dares and post the results online under the guise of some game challenge. Do not give in to such provocation and/or challenge. Stop playing such games and inform your parents/ elders.

c) Many adults and cyber criminals pretend to be children while playing online games. They may try to befriend you by giving tips about the games, sharing points with you and trying to win your trust. They may use this opportunity to get your personal information or influencing you for a one-to-one meeting.

d) Some games may have content which might upset you. This could include violence, horror, or sex or induce you to self-harm. Do not play these games and talk to an adult if you are upset.

e) Online games are sedentary in nature and children can be involved for long periods without moving around. It is good advice to take breaks every hour or alternate online games with outdoor activities.

f) Be aware of when you feel like you might be getting addicted to online gaming. Check if your online games, stop you from seeing your friends or family

i) take the place of doing homework
ii)make it hard to stop thinking about playing
iii) make you unable to stop playing, even when you need to sleep

If you feel this is happening, it's a good idea to get support. Talking to someone you trust, preferably an adult or a professional counsellor. Either they may be able to help or help you find someone who can help.

Know the risks, exercise good judgment and seek advice. What you do online has the potential to affect everyone – at home, at school and around the world. Practicing responsible online habits benefits the digital community.

## *3.3 Safety and security during online gaming*

You need to be careful and follow safeguards to protect yourself and your friends from potential risks associated with online gaming. You may end-up downloading viruses and malwares which can compromise the security of your computer or smartphone. You do not know other players and their intentions. The personal information shared by you can be misused by scammers or cyber bullies. Some cyber criminals befriend children by helping them with winning games or sharing points. They may win your trust and later ask for your help to buy coins/points, etc.

***Good practices: How you can protect yourself while playing games online***

***Prudent selection of games to play***

a) Check the age classification of the games you want to play. Stick to the ones that have been indicated for your age group.

b) Never install games downloaded from free online gaming websites that are not reputed. Never download games by clicking on links received on mail or text message or through a pop up.

***Protect personal information***

a) Always install a good antivirus software on your computer, smartphone or other handheld devices. Regularly update the antivirus and other applications.

b) Do not share personal information like name, date of birth, address or phone numbers while playing online games.
Never share your passwords with anyone. You should use a complex password for your online gaming account and other online accounts. It is a good practice to change your password at regular intervals.

c) Never use voice chat or webcam while playing online games. This may share your identity with other players and attract cyber bullies and other cyber criminals.

d) Never share your or your parent's credit card/debit card details with anyone when you are playing online games. They may ask credit or debit card details. Never share such details with anyone.

***Know how to respond to online challenges***

a) Know the tools that are available to deal with aggressive or inappropriate conduct online. Learn how to block, mute, delete and report on the games and consoles being used.

b) If you face any challenge in online gaming world, immediately inform your parents or elders so that they can support and guide you.

c) Never meet in person with someone from your online gaming world. In real/life they may be very different. Cyber criminals may befriend you and try meeting you or getting your personal information. They may have wrong intentions.

Balance online gaming and playing outdoor games. You will enjoy outdoor activities, this is good for your health and you can meet real friends and enjoy their company.

***Limits in friendships***

Relationships are complex and privacy is personal. Set limits to your online friendships as well as online communication with real life friends. There has to be a limit to what you share or exchange in terms of written words, photographs or videos. Remember, once online, you may not be able to control who will actually see it, prevent breach of trust and misuse and potential risk and harm to your person and reputation.

A class 8th girl's Instagram account was hacked by one of her classmates. He used her account to send obscene messages and videos to her friends and also to all the people who were added in her account. Next day her friends didn't talk to her nicely and those who talked were very indifferent (rude) in their behavior. The girl did not understand the situation and this kept on happening for a week. The girl was in despair and asked one of her friend as to why is everybody avoiding her. To her surprise, she had no clue that this all happened. She then clarified with her friends and sorted her problem.

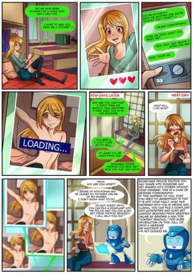
The problem that still remains is that her account is still being used by someone even though most of her friends have reported that account.

Learnings: Always make sure that you use Strong Passwords and not reveal to anybody, even your best friends. Make sure that if something like this happens, you tell it to your parents, elders, and teachers. Also in such cases report to cybercrime branch of the police

There have been many cases of revenge porn in recent years that highlight the importance of limits to offline and online friendship.

***Revenge pornography*** is "An act whereby the perpetrator satisfies his anger and frustration for a broken relationship through publicising false, sexually provocative portrayal of his/her victim, by misusing the information that he may have known naturally and that he may have stored in his personal computer, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to defame the victim."[6]

Teenagers in the age-group of 14 to 18 years are the worst victims of revenge porn as well as the perpetrators themselves, which is a matter of concern.[7] Some teenage students who have been in a relationship and end it find their explicit photographs circulated on social media platforms or tags her in the pictures or sends her a link. When such images go viral, students are often harassed and bullied by their peers – branded with instability and in the end, isolated. A teenager may be targeted by her jealous classmates, her ex-boyfriend or even an unknown friend on social media who may be victimising her because she stopped communicating with him when she realised the dangers of online relationships.


SO WE HAVE BEEN TALKING FOR A WHILE NOW, AND I LIKE YOU.
I WANT TO SEE YOU. SEND ME A PICTURE? :)
YOU'RE SO PRETTY. SEND ME ANOTHER ONE MAYBE WITHOUT THAT T-SHIRT? ;)
I'M NOT COMFORTABLE.
COME ON PRIYA. DON'T YOU TRUST ME?
HUH. OKAY. BUT DELETE IT AFTER YOU SEE.
SURE. TRUST ME.
LOADING...
FEW DAYS LATER
WHY ARE YOU LIKE THIS? I DON'T THINK WE SHOULD TALK ANYMORE. I THINK WANT YOU IN MY LIFE ANYMORE.
YOU @$#'&. I DON'T CARE. GO TO HELL.
AT LEAST I'LL BE AWAY FROM YOU
REMEMBER THOSE PHOTOS YOU SENT ME? NOW YOU WAIT AND WATCH
NEXT DAY
WHAT WILL I DO NOW?
PRIYA, WHY ARE YOU UPSET?
I BROKE UP WITH ROHAN AND HE LEAKED MY PICTURES ONLINE. IM SO SCARED. I DON'T KNOW WHAT TO DO.
DO NOT WORRY PRIYA. YOU CAN FILE A COMPLAINT WITH THE POLICE AND YOU CAN ALSO GET THESE PHOTOS REMOVED. I WILL HELP YOU OUT."
SOMETIMES PRIVATE PHOTOS YOU MAY SHARE WITH SOMEONE MAY GET SHARED WITH OTHERS WITHOUT YOUR CONSENT. THIS IS A CASE OF REVENGE PORNOGRAPHY. IF THIS HAPPENS TO YOU, WHAT YOU NEED TO UNDERSTAND IS THAT IT IS NOT YOUR FAULT. WHAT HAS HAPPENED WITH YOU IS WRONG AND ILLEGAL. YOU CAN FILE A COMPLAINT WITH AUTHORITIES AND ALSO GET CONTENT REMOVED FROM WEBSITES ONLINE BY SENDING A MAIL FOR "CONTENT REMOVAL." FOR MORE INFORMATION ON THIS, CALL OR DROP A MESSAGE ON WHATSAPP AT +91 957 00000 66.

6 *Halder, Debarati and Jaishankar K in the International Annals of Criminology, 2013. https://www.parentcircle.com/article/protect-your-child-from-revenge-porn/*

7 *Halder, Debarati. Professor of legal studies at Karnavati University.*

This can lead to students dropping out of schools and preferring to stay home or change schools. This pushes them into depression and isolation from their friends. Often, students don't report such cases to their parents and their teachers fearing that the issue will blow up into something big, which lands them into more problems.

While some teenagers may know the dangers of sexting, peer pressure forces them to indulge in this as due to peer pressure and not wanting to be left out of the group. Children should not succumb to peer pressure, especially to take risks of this kind which can be extremely embarrassing and damage their reputation. In extreme cases children have been driven to suicide. Do not give in to pressure. If you lose your inhibitions you also lose control. Once you have pressed the enter key you cannot retrieve your message and may make yourself vulnerable to potential harm and exploitation.

However, teenagers need to understand gender relations. Boys must learn to interact with girls on equal terms and respect them and their desires as those of human beings, not simply as objects of respect or desires. Consent must be an important part of relationships. Pictures, videos and other material shared in confidence cannot be published on social media without the permission of the person just because the other person does not want to continue in the relationship. Youngsters must learn to cope with rejection as it is a part of life but not the end of the world.

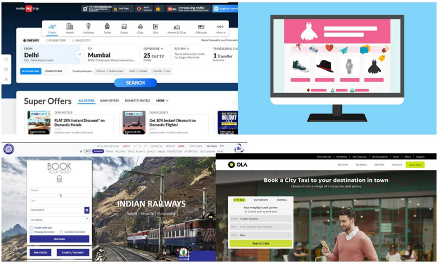
WATCH

*https://www.youtube.com/watch?v=0AxfdpuyHS4*

## 4. Digital Commerce

### *4.1 What is digital commerce?*

Digital commerce is about the users undertaking legitimate and legal exchanges using digital technologies. The new digital economy has improved the choices of goods and services to the consumers. They can choose what they want from a wide array of products offered by an ever expanding market of online vendors. The virtual market place is assisted by a growing network of financial and other service providers.


make my trip
Delhi
Mumbai
25 Oct'19
1 Traveller
SEARCH
Super Offers
FLAT 28% Instant Discount* on Domestic Hotels
Get 10% Instant Discount on Domestic Flights!
BOOK YOUR TICKET
INDIAN RAILWAYS
Safety | Security | Punctuality
OLA
Book a City Taxi to your destination in town
Choose from a range of categories and prices
Search Cabs

Websites provide outlets for sales of goods and services. A growing number of brands are available online to consumers directly through their own platforms or through aggregators.

a) Buy and sell (e.g., Amazon, Flipkart, eBay, Facebook "marketplace",...)
b) Book travel (e.g., IRCTC, MakemyTrip, RedBus.in, booking.com)
c) Book hotels (e.g., Trivago)
d) Order food (e.g., Zomato, Swiggy,)
e) Sell used products (e.g. Olx, Quikr, ebay,)
f) Make payments (Paytm, Google Pay, Bhim, UPI, credit and debit cards, and netbanking)
g) Advertise goods and services
h) Pay taxes (e-payment portals)

**Good practices**

*• Install a robust anti-malware and antivirus solution*
*• Be extra careful while visiting websites that ask for personal and financial information*
*• Never click on suspicious email messages, especially those offering loans and too good to be true deals.*
*• Shop only at websites you trust. Check the security features of new websites and the authenticity and customer reviews of the business.*
*• Keep the receipt, order confirmation number, and postal tracking number safe.*
*• Report if you do not receive merchandise of the promised quality.*

### *4.2 Opportunities and risks*

An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It's also called an electronic payment system or online payment system. The electronic payment system has grown increasingly over the last decades due to the growing spread of internet-based banking and shopping. Technological advances are bound to increase the use of electronic payment systems and payment processing devices. As these increase, improve, and provide ever more secure online payment transactions the percentage of check and cash transactions will decrease.

***https://securionpay.com/blog/e-payment-system/***

But you are also susceptible to financial frauds, involving privacy breach, identity theft, unauthorised access and siphoning of money.

***Cybercrime***

In Phishing and Vishing. A target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Phishing is a cybercrime in which a website's traffic is manipulated and confidential information is stolen.

Vishing is the telephone equivalent of phishing. It is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

Pharming is essentially a phishing scam that infects multiple users at once. It exploits the foundation of how Internet browsing works — namely, that the sequence of letters that form an Internet address, such as www.google.com, have to be converted into an IP address by a DNS server in order for the connection to proceed.

This exploit attacks this process in one of two ways. First, a hacker may install a virus or Trojan on a user's computer that changes the computer's hosts file to direct traffic away from its intended target, and toward a fake website instead. Second, the hacker may instead poison a DNS server, causing multiple users to inadvertently visit the fake site. The fake websites can be used to install viruses or Trojans on the user's computer, or they could be an attempt to collect personal and financial information for use in identity theft. In cases of DNS server poisoning, the affected user can have a completely malware-free computer and still become a victim. Even taking precautions such as manually entering in the website address or always using trusted bookmarks isn't enough, because the misdirection happens after the computer sends a connection request.

***Malvertising*** It is the process of using advertisements to infect your devices and systems with malware. These ads look legitimate and trustworthy, by one simple click will cause your phones and computers to be compromised.

***Piracy.*** Production and consumption of pirated music, software, Games and videos is common but illegal.

An equal amount of goods and services which are in conflict with the laws or morals of some countries are surfacing (e.g., illegal downloading, pornography, and gambling)

## *4.3 Safety and security measures for online transactions*

### *4.3.1 General safety measures*

Secure your digital devices linked with bank accounts with strong passwords and good antivirus software. Choose unique, non-guessable and meaningless passwords.

Secure your bank accounts, credit and debit cards using strong passwords and features like 2 - factor authentication and login alerts. Update the online passwords of bank accounts and the PIN of debit and credit cards regularly. Do not share online account password, card number, CVV, expiry date, PIN and OTP with anyone.

Computers in cyber cafes may not have updated antivirus or may be infected with malware, which may compromise your bank details and other sensitive information such as card number, expiry date, CVV, etc.

a) Avoid making online financial transactions using a public Wi-Fi or a computer in a cyber cafe.

b) Learn to create a VPN or Virtual Private Network, which is encrypted to allow safe and secure communication over an unsecure network.

### *4.3.2 Prevention of financial frauds*

Online vendors or service providers as part of their verification process often ask for personal information, including address, email address, previous addresses, mother's maiden name, place of birth, pin number, bank account details, Aadhaar number and passwords.

Such information is also required by cyber criminals for unauthorised and illegal transactions. By getting hold of some information, they can access other information about the potential victim and make unauthorized financial transactions using the victim's credit card or bank account, commit other crimes, such as entering (or exiting) a country illegally, trafficking drugs, smuggling other substances, committing cyber-crimes, laundering money and much more. In fact, they can use the victim's identity to commit almost any crime imaginable in his or her name.

If a criminal has used another person's identity to commit a crime, this can put the victim under police suspicion. The victim may find themselves being investigated as part of a criminal investigation, and in some cases they may find it difficult to prove their innocence.

a) Disconnect the phone after receiving any call from anyone claiming to be a service provider, who seeks sensitive information to avoid deactivation of your number or making a just too generous offer. Immediately call customer care to check if such a call is genuine.

b) Always type in the bank website when trying to login to the bank account. Do not not click on a link to the bank website, which appears on an email, text message or a pop-up. This may be a fake link and may take you to a fake site. Once you login to your bank account from a fake site, your sensitive details like account number and password may be stolen.

c) Check for the bank's security certificate details and various signs such as green address line, lock sign on the address bar and HTTPS to confirm the security of the bank's website.

d) Review monthly statements of bank account and credit cards carefully to check if there are any transactions you do not recall.

e) As soon as you discover bank account or credit card transactions not made by you or lose your debit or credit card, inform the bank immediately and get you card and account blocked, and follow up by lodging a formal complaint at the nearest police station.

**RBI Guidelines regarding protection against financial frauds**

*https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11040&Mode=0*

Scan QR Code to read the Guidelines

***Identity Theft*** If anyone uses any information that is unique to you to impersonate you without your consent, it is called identity theft and is illegal.

***Hacking*** It is the process of gaining access to a system or account without authorization.

***Malware*** Short for malicious software, these are software that are designed with the intent to disrupt, damage, or gain unauthorized access to a computer system.

***Ransomware*** A specific kind of software that blocks the user from accessing their devices/systems until a ransom is paid.

***Be cautious with links:*** If you get an email or notification that you find suspicious, don't click on its links. It could be a phishing attack. It's always better to type a website's address directly into a browser than clicking on a link.

***Watch out for typographical errors:*** Phishing scams are infamous for having typos. If you receive an email or notification from a reputable company, it should not contain typos.

**Take a phishing IQ test to see if you can spot a fake email**

*http://www.komando.com/tips/361345/-
can-you-spot-a-fake-email-take-our-phishing-iq-test*

Scan QR Code to take the test

### *4.3.3 Cautious browsing*

If the website looks strange, the address in the address bar looks off, or the site starts asking for information that it normally doesn't, check to ensure there is a lock icon in the address bar, denoting a secure website, and click on the lock to ensure that the website has a trusted, up-to-date certificate. Those running DNS servers have some pretty sophisticated anti-pharming techniques at their disposal, but the risk of being hacked is always there, so you can only mitigate the risks through a combination of personal protection and Internet awareness.

### *4.3.4 Online purchases and sales*

a) Download only from verified and secure sources like PlayStore and AppStore. Downloading from other sources may lead to your devices being infected by malware.

b) Resist the temptation to open emails and attachments from unknown sources, especially those offering special deals or surprises.

c) Some offers may be too good to be true. Beware of such offers as they may be fraudulent.

d) Compare the prices of the product at different sites to avoid being overcharged.

e) Make payment only after you have verified the buyer and the products.

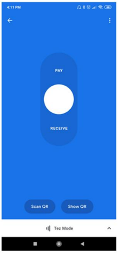
Some sites facilitate the sale of old and used products. Just in case you decide to avail of this facility, ensure that the ad you post has all the necessary details about the product.

a) Exchange financial details only if absolutely necessary.

b) Verify the details of the buyer by asking them to produce a valid government id.

c) Meet the prospective buyer at a public place for your own safety.

d) Test the functioning of the items like electronic goods, cars and vehicles.



5:53 PM
[redacted]
Paytm Wallet Linked to [redacted]
₹ 100
Add Message
Money will be sent from your Paytm Wallet
Pay

**Hazards of providing sensitive information online (credit, debit card info, sharing OTPs, account numbers, etc)**

Some of you may be using banking services such as debit card, credit card, net banking, etc. at this stage but as you grow up many more may start using these services. As a smart citizen you must understand how online transaction frauds can happen so that you can be safe yourself, teach others in your family and friend circle.

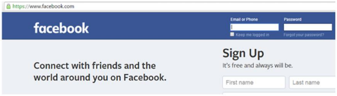
**Cyber criminals cheat people online in many ways.**

They may send an email to a bank account or credit card holder from a fake account, which appears to be from their bank or credit card service provider. The unsuspecting user who clicks on the link provided in the email is taken to a page where he or she is asked to share details of the bank account or card, card verification value and expiry date. Once such sensitive information is shared, their bank or credit card account is seriously compromised.

Posing as a bank employee, they may try to obtain credit card or bank details such as account number, personal identification number (PIN), CVV, expiry date and date of birth. Once such details have been provided, the account is seriously compromised. As mobile numbers are usually linked with bank accounts, posing as an employee of the mobile service provider they may call and inform the user that his or her mobile number will be disconnected if they do not update their Subscriber Identification Module (SIM). They attempt to make the user to click on a link or send an SMS to a number shared by them. They claim that the link and number will connect the user with the service provider but are actually trying to establish a connection with a duplicate SIM obtained fraudulently from service provider. If the unsuspecting user falls in the trap, they use the duplicate SIM to transact online using the victim's mobile number and banking app.

The victims of such financial frauds experience serious problems. They end up being saddled with debts for monetary transactions they have not done. In order to avoid liability for debt repayment, they have to provide proof that they have indeed been duped. The process can be difficult and time-consuming.

***Check the website URL. HTTPS encrypts your data in the website and protects it from any kind of tampering. Do not share your confidential information such as online account password, card number, CVV, expiry date, PIN and OTP on the website which does not start with HTTPS.***


https://www.facebook.com

facebook

Email or Phone | Password

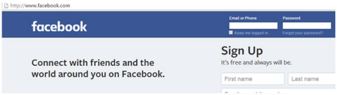
Keep me logged in | Forgot your password?

Connect with friends and the world around you on Facebook.

Sign Up

It's free and always will be.

First name | Last name


http://www.facebook.com

facebook

Email or Phone | Password

Keep me logged in | Forgot your password?

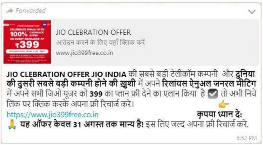
Connect with friends and the world around you on Facebook.

Sign Up

It's free and always will be.

First name | Last name

***Messages claiming you have won prizes***


Forwarded

JIO CLEBRATION OFFER

आवेदन करने के लिए यहाँ क्लिक करें

www.jio399free.co.in

**JIO CLEBRATION OFFER JIO INDIA** की सबसे बड़ी टेलीकॉम कम्पनी और **दुनिया की दुसरी सबसे बड़ी कम्पनी होने की ख़ुशी** में अपने **रिलांयस ऐनुअल जनरल मीटिग** में अपने सभी जिओ यूजर को **399** का प्लान फ्री देने का एलान किया है ✅ तो अभी निचे लिंक पर क्लिक करके अपना फ्री रिचार्ज करे। 👉

https://www.jio399free.co.in

**कृपया ध्यान दे:**

🙏 **यह ऑफर केवल 31 अगस्त तक मान्य है!** इस लिए जल्द अपना फ्री रिचार्ज करे.

6:52 PM

***Scams using IDs of Army officials.***

# 5. Digital Etiquette

***5.1 What is digital etiquette?***

Digital etiquette is about being aware of and behaving in an appropriate, responsible and ethical manner while using digital devices and technology. This includes shaping your digital reputation and being a responsible citizen of the communities in which you participate, from school groups, to games, to social networks.

Etiquettes in our real lives and the virtual world are similar - be thoughtful, considerate and polite online just as you would be offline. What works in real life also works in the virtual world. Well almost. It is easier to detect strangers in real life than in the virtual world.

If you have witnessed cruel or inappropriate behaviour on social networks, it does not give you the license to do the same. Or if someone has bullied you it is not an excuse for you to repeat the bad behaviour to someone else.

**Golden rules**

- *Be positive in your online behaviour*
- *Treat others online the way you wish to be treated*
- *Learn to say and accept "No"*
- *Do not post anything that you would not like to last forever*

***5.2 Offline etiquettes are also online etiquettes***

Sometimes children use digital devices and technology in the wrong context. For example:

*a) Using mobile phones while talking to someone constitutes a social faux pas or even an insult to the other person.*
*b) Texting while carrying on a conversation with someone is very rude and shows disrespect.*
*c) Using mobile phones in classrooms, meetings and social gatherings. Using cell phones to text while attending a class is not appropriate.*
*d) Ping others late at night. There is a time for everything. Do not disturb others at night. You may also not like to be disturbed when you are trying to rest.*
*e) Playing audios and videos loudly in public. It is rude and inconsiderate to others.*

**Agree to disagree.** Make respectfully disagreeing the norm. Respect the opinions of your classmates. If you feel the need to disagree, do so respectfully and acknowledge the valid points in your classmate's argument. Acknowledge that others are entitled to have their own perspective on the issue.

**Avoid digital drama.** "Digital drama" in the form of hurtful comments, mean-spirited rumours, and embarrassing photos, is a pretty common online occurrence. Such posts spread quickly and cause immense harm to someone. Perception of anonymity may give a false sense of complacency and false bravado. Lack of sensitivity or thought can impacts friend-ships and creates unnecessary and avoidable tension in the network and community. Just think how you would feel if the same happened to you.

**Treat others online the way you wish to be treated. Before posting, ask yourself:**

- ***Would you say that to someone's face?***
- ***How would it make the person feel?***
- ***Could someone take your message the wrong way?***
- ***Will this hurt someone's reputation?***
- ***How would you feel if someone said that to you or wrote that about you?***
- ***Would you want your friends, parents or teachers to read this about you?***

It is easier to say hurtful or disrespectful things without standing face-to-face with someone, however, it is important to remember that your classmates and teachers are real people who are affected by the words you say and write. It is essential to keep in mind the feelings and opinions of others, even if they differ from your own. ***If you wouldn't say it to someone's face, don't say it online either.***

If you feel hurt after reading a post from a friend or a stranger, do not react with an aggressive reply. If hurtful post or message is from a friend, request him not to do it again. If you are repeatedly getting such messages/ post, please inform your parents or elders immediately so that they can support you.

Also, please remember that as a good digital citizen you should not share mean comments or hurtful messages or embarrassing pictures/videos online. Please be careful and check if your post/comment /videos can be embarrassing for your friend or anyone else. If so, please don't post.

### *5.3 Being positive online*

Students are encouraged to take an active role in building positive, supportive online communities. Here are some things you can do to contribute to a positive online environment.

#### *5.3.1 Posting positive*

As a responsible digital citizen, always review your messages and posts to be sure that they are not untruthful, negative, sarcastic or rude.

#### *5.3.2 Being responsible, honest and truthful*

Misleading others is a major breach of online etiquette. This is true even if it is unintentional.

Check facts before providing information or giving advice online. Misinformation will just add to the clutter of the internet and waste people's time.

Avoid posting anything that is not true such as rumours or gossip.

So do not be naive and forward that message hoping it will bring you good luck. Many viruses are spread via chain messages and invitations. If you wish to forward information, make sure it is verified and shared with people you know.

**Check the accuracy of your messages**

Forwarding messages without checking their accuracy: This may contribute to the phenomenon of "fake news" and rumor mongering.

Double check messages before hitting the send key. Pause and think about your posts, comments and e-mails before you send it. Once you press the send key, there is no way to take back the messages. Sometimes a message that is meant to be funny, may not come off that way at all because the person on the other end cannot see your facial expressions or hear the tone of your voice. Read your messages again to see if they can be misunderstood. It is best to discuss sensitive or difficult issues with the person directly rather than posting something online or sending a hurtful e-mail.

### *5.3.3 Respecting people's confidence*

The ability to keep information shared by someone in confidence reflects a strong character. Do not reveal the information online (or off-line) if the answers to the following questions was "yes".

- Was this information supposed to be confidential?
- Will it embarrass the source of information?
- Will sharing this information compromise someone's privacy or create drama?

If the answer to these questions is "yes", do not reveal the information. That is what a good friend would do.

Always ask permission before uploading someone's pictures and posting personal details. It constitutes a violation of the privacy of the person whose pictures or personal details have been posted.

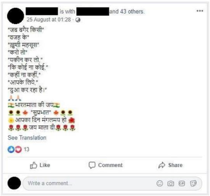
Cluttering other peoples' inboxes, which annoys most people. Tagging your friends may seem harmless but it is important to get their consent. Everyone does not see things the same way and you may strain your relationship.

### *5.3.4 Knowing boundaries*

**Do not post anything that you do not want to last forever.** Before you say or post anything online, ask yourself, "Am I ok if this is never deleted? Once something is posted online, it is likely to be there forever. As of now, there is no delete button or eraser for the Internet.

**Avoid inappropriate use of technology.** Users have a responsibility to use technology appropriately without harming or inconveniencing others. Many users often use technology inappropriately without understanding the consequences. For example

**Spamming** is the sending of unwanted bulk messages indiscriminately through emails, internet forums, instant messaging, social networks, mobile text messaging, fax transmission, advertisements, and other networks.


[redacted] is with [redacted] and 43 others.
25 August at 01:28 ·

*जब बगैर किसी*
*वजह के*
*ख़ुशी महसूस*
*करो तो*
*यकीन कर लो,*
*कि कोई ना कोई,*
*कहीं ना कहीं,*
*आपके लिये,*
*दुआ कर रहा है।*
🙏🙏
🇮🇳भारतमाता की जय🇮🇳
🌻🌻🍁 *सुप्रभात* 🍁🌻🌻
🌞 आपका दिन मंगलमय हो 🌺
🌹🌹🌹जय माता दी🌹🌹🌹

## 5.4 *Cyberbullying and cyberstalking*

A fine line separates bullying from teasing. Different people have a different threshold of tolerance for being able to take teasing or cyberbullying. Know and understand what cyberbullying is and never engage in that kind of behaviour.

**Teasing versus bullying**

a) Teasing typically happens among friends or kids trying to fit in with their peers

b) When it goes back and forth equally between kids, it's usually playful. If one person asks for it to stop, the other does so.

c) For adolescent boys, teasing is a "rite of passage". Teasing can get rough, but it's not meant to hurt the other person.

d) A bully fully intends to harm his or her victim and has the power and the means to do so. This person might be more popular or physically stronger, and the victim may have a hard time defending himself.

e) Children who are seen as different or don't "fit in" are typical targets of bullying. This includes children who have a disability, are overweight, or are thought to be homosexual.

**Unacceptable use of technology to bully others**

Being at the receiving end of offline or online bullying can be very distressing for anyone. Under no circumstances can such behavior be considered acceptable.

**Various forms of cyberbullying**

- *Making fun of another user in internet chat rooms*
- *Harassing a user over instant messaging sessions*
- *Posting derogatory messages on a user's social networking pages*
- *Circulating rumours about another on social networking sites.*
- *Publishing lewd comments about another person on personal blogs*
- *Posting unflattering pictures of another user on the web*
- *Sending unsolicited and unwanted email messages (also known as spamming).*
- *Sending threatening or provocative emails*
- *Repeatedly calling another person's cell phone*

"**Trolling** is also a type of cyberbullying, where repeatedly harassing or intimidating comments are made.

The cyberbullies can be known people, known people hiding their identities, or strangers who use digital technologies to send nasty text messages or emails, or set up hate groups on social networking sites. The victim is often targeted constantly or periodically even when they are in the comfort of their own home. The technologies enable them to circulate messages or images very quickly and widely on the internet, which makes it very hard to combat cyberbullying. Cyberbullying takes place between two young people.

***How to deal with cyberbullying?***

***Prevent cyberbullying***

a) Do not accept friend requests from unknown people on social media platforms. A cyberbully can even create a fake account to befriend children. As a rule of thumb, only add people online who you know offline.

b) Remember what you post online remains there, so do not share your personal information like date of birth, address, and phone number on social media or other online platforms. You can go to privacy settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only.

c) Do not install unwanted software and apps like dating App, online games, etc. from unknown sources. Be careful of revealing personal details or identity details if using common spaces for online interactions.

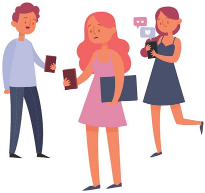
d) If you feel upset after reading a post from a friend or a stranger, do not react with an aggressive reply. Resist the urge to retaliate or respond immediately. It may encourage the bully to keep posting such messages. Take a break and do something you enjoy doing to distract yourself.

e) Convey your discomfort to friends and acquaintances about hurtful posts or messages they may have shared or sent with unequivocal request to not to do it again. If such posts and messages persist, inform your parents or trusted elders immediately so that they can support you.

f) Block and if need be report using the site's reporting function as soon as possible if someone makes you uncomfortable on a social networking site.

**Cyberstalking** is when an individual is repeatedly or constantly followed, watched or contacted through any electronic means. The movement of the child is tracked and privacy is invaded or persistent efforts are made to contact someone against their will through text, email, social media, or other digital platforms.

Cyberstalking a child may be directed at sexually harassing a child or for other mala fide motives. It could be done by an adult or an older child.


*Singling out someone online, using offensive gestures or employing offensive language, posting a meme or joke about someone...*

**Causing harm to somebody unintentionally through the use of technology**

**Unintentional harm:** cyberbullying has an adverse effect on the victim and can cause emotional and psychological problems. Victims can experience stigmas, shame and humiliation from peers. Often they may report headaches, stomach aches that often accompany nervousness and anxiety. They may also turn to self-harm in different ways. Being bullied can lead to low self-esteem and poor performance in school. In some cases it can lead to depression with some children feeling hopeless and helpless about their lives. In extreme cases it can lead to suicide by the victim.

**Just think.** Would you like to be at the receiving end for these possible consequences, even if these are unintentional? Consider the possible impact of your online actions. You may cause a lot of harm to the child which can have a long term impact on personal well being as well as school performance. Will you be comfortable being responsible for any of this?

**What to do when you realise you are experiencing the impact of cyberbullying /cyberstalking?**

If a child has been the victim of cyberbullying or cyberstalking and/or is experiencing any of the signs of harm described above, the child must immediately inform a trusted adult, either parent, teacher, counsellor or relative. They will initiate the actions required for addressing the offender as well as take measures to provide help for coping with the ill effects. This is in your interest; do not remain quiet about it. Remaining quiet will give the offender confidence to trouble other children as well. At the same time you will ignore your need for help and assistance to cope with the situation.

*A class 10th girl was getting lewd phone calls and messages from some anonymous number. She was afraid to tell it to her parents because she knew her dad had a loose temper and he will try to harm that anonymous caller by tracking him down by hook or by crook. With this fear in her mind she didn't bother to complain. The phone calls and messages didn't stop. She started fearing that the boy can follow her too and sooner did this happen. Wherever she went, he started following her, be it her tuition classes, be it some outing spot. The situation became worse when he started clicking her pictures. The girl was frightened and she dared to complain to the cybercrime branch.*

*Lesson: Always tell your parents or a trusted adult if someone is troubling you. They would be able to help you. Take the screenshots of such chats as proof, which can be shared with the police authorities.*

*A girl of class 9th was abused and threatened by a relative. She was tortured and sometimes even drugged. The relative used to send her abusive messages and threaten her that he will tell her parents that she has a boyfriend. She was scared to confide in her parents because of the fear that her parents would not believe her.*

*Lesson: Keeping silent is not a solution to such a problem. Never be scared of telling your parents the truth. Make sure to complain about such problems to the police and seek help from authorities whenever needed. There are people willing to listen to you and help in addressing your problems.*

*A 7th standard girl was blackmailed by an adult who kept on asking the girl for her nude pictures. She explicitly refused every time he asked and blocked the person. The blackmailer hacked one of her social media accounts and took her photos and just to take the revenge he morphed her photos and posted them online. The girl was embarrassed, agitated and even thought of committing a suicide.*

*Lesson: Be strong and face the situation wisely. Do not be afraid of such offenders. Report such crimes on the platforms, cybercrime branches, authorities who work for child development, child helpline. Do not think of yourself as a victim.*

### 5.5 Teacher abuse by children

A recent trend observed is that children some children are taking to online platforms to take revenge on their teachers either by posting derogatory comments with the name of the teacher in a group, starting a discussion about them which attracts other negative comments, posting explicit pictures or stalking either by impersonating someone or through unauthorized access to teachers devices. All these activities are unethical and against digital etiquette and at the same time, several of these may attract legal consequences.

If students have issues concerning their teachers, which are bothering them, they should approach the school administration rather than resort to such measures that can get them into serious trouble.

### *5.6 Online reputation and digital footprints*

Internet users leave behind "digital footprints", which can influence their reputation. It is made up of the content created, posted and shared by the user, as well as the content posted and shared by others with and about the user. It is made up of information on websites they visit, emails they send, any information they submit online, and posts on social media platforms. It can be positive or negative and affects how people see the user now or in the future. So it is important that you know what kind of trail you are leaving, and what the possible effects of this trail can be.

***Harvard university case***

*Kyle Kashuv, a recent graduate of a high school in Parkland, Florida in the US gained initial notoriety as an outspoken advocate against gun control in the wake of the 2018 Parkland attack that left 17 dead. He had survived the incident but unlike many of his classmates who demanded stricter gun control measures, he argued for maintaining strong Second Amendment rights and successfully lobbied for the federal STOP School Violence Act, which included several school safety measures in lieu of stricter gun control measures. According to his classmates, he was prone to expressing vile, blatantly sexist and racist views in person, texts and shared google document. Not only did Kashuv become something of a celebrity, he also was very academically accomplished and won admission to Harvard.*

*But in May, the Huffington Post released a series of vile, blatantly racist slurs made by Kashuv after receiving them from Parkland students. Although Kashuv attempted to delete the document, it was too late. He posted a Twitter explanation for what he called "callous comments I made a few years ago," claiming "we were 16-year olds making idiotic comments, using callous and inflammatory language in an effort to be as extreme and shocking as possible. I'm embarrassed by it, but I want to be clear that the comments I made are not indicative of who I am or who I've become in the years since."*

*Almost immediately, Harvard launched an investigation, including contacting Kashuv for an explanation and informing him that it reserved the right to withdraw offers of admission in situations where students behave in ways that "brings into question your honesty, maturity or moral character." Kashuv sent a letter of formal apology to Harvard, but the university decided to rescind his admission and rejected his appeal against its decision on the basis of reports and his written sentiments.*

*The reaction to Harvard's decision to withdraw its offer of admission to Kashuv was strong and loud. One perspective was that a liberal institution treating a conservative youth unfairly. After all, he was only 16 when he stated his racist views and had subsequently apologized. The other perspective defended Harvard's decision as a proper and necessary institutional rejection of racism. College admissions are premised on the behaviour of young people. As a private university, Harvard has every right to decide which students will be admitted.*

*Based on media reports*

Make a positive footprint: The best way to keep your online reputation in check is to use your time online to get creative and create a positive footprint. For example, why not write a blog to promote all the great things you are doing, fundraise for a charity using an online sponsorship page or create a video to teach others something new.

Many social media platforms offer insights into the personality traits to the users. Their interest is expressed once they accept the offer or take a related quiz. They give their consent in this process or their consent is deemed. The social media platform and/or the app developer are able to use the information trail left by the user to offer them the results. This is indicative of the amount of information about the users that the social media platforms possess.

**Protect Your Online Reputation**

Use the simple checklist to help manage and maintain your online reputation.

**Search Yourself Online:** Do you know what information about you is available online? Do a simple web search of your name and see what you can find. If you find something you are not happy with, take the necessary steps to get that content removed. Remember if your Facebook or Twitter pages appear you can change this by adjusting your privacy settings.

**Check Privacy Settings:** Make sure you know what information you are sharing on the websites you use, in particular on social networking sites. Most social networking sites have privacy settings to help you manage the content you share and who you share it with; you can decide if you want your posts to be shared with your online friends and followers only or with the public. Keep in mind that your friend's content and their settings can also affect your digital footprint.

***Think before you post***

*Before you post that funny picture of your friend, or make that joke about someone on Twitter, ask yourself do you want everyone to see it; friends, family, grandparents, future employers? Would you be happy for others to post that type of content about you? You should be proud of everything you post online, remember once it is online it could potentially be there forever!*

**Deactivate and delete:** when you stop using a social networking profile or website, it's a good idea to deactivate or delete your account. This will mean the content is no longer live and should not be searchable online; it will also remove the risk of these accounts being hacked without you knowing.

Cambridge Analytica came under media glare and public scrutiny when it was revealed that it was selling psychological data to candidates in the US Presidential election. The revelations have placed the practices and responsibilities of Facebook and other companies under intense scrutiny, and raise questions regarding the responsibility of the Internet industry.

***Cambridge Analytica case and its implications for data privacy***

*Political data firm Cambridge Analytica obtained the data of 50 million Facebook users, constructed 30 million personality profiles, and sold the data to US politicians seeking election to influence voters, without the users' consent. The following are some facts of the case.*

*A Cambridge University researcher developed an app called 'thisismydigitallife' in 2014. The users had to consent to give the app access to their Facebook profiles and those of their friends in order to take the quiz. They were to receive $1-$2 to take the quiz, which was advertised to remote freelance workers on Mechanical Turk, a crowdsourcing online marketplace controlled by Amazon.*

*Over 270,000 users took the quiz. But the app was able to access the full profile of over 50 million friends' accounts – which, at the time, Facebook's API (application programme interface, i.e., the platform for building applications) allowed by default. The researcher obtained a licence from Facebook to harvest such data through its API 'for research purposes only'. But he violated this agreement by giving the data to political data firm Cambridge Analytica, which was co-founded by a donor to the Republican Party in the US, and which reportedly paid him $7 million for his efforts.*

*Cambridge Analytica matched the data of 30 million users (out of the original 50 million) with other records to construct personality profiles on millions of American voters. It classified voters using five personality traits - openness, conscientiousness, extraversion, agreeableness, and neuroticism (OCEAN) to identify the personalities of American voters and influence their behaviour, using psychographic modelling techniques.*

*In December 2015, the media found out that Cambridge Analytica had sold psychological data to a candidate in the US presidential campaign. It was reported that Facebook claimed that it had removed the app once it learned of the violation of platform policies. But did not clarify what it did with the information that had already been gathered. The researcher, Cambridge Analytica, and one of its former employees certified to Facebook that they had deleted the data. But Cambridge Analytica continued to sell the data to another candidate.*

*The investigations are going on with allegations of Russian interference in the US election and ties with the group behind the UK's Leave EU campaign (Brexit) in 2016. It has been reported that a large amount of the data is still on the company's servers even though it is not clear how much the data actually contributed to influencing voters.*

***https://dig.watch/trends/cambridge-analytica***

WATCH

***https://www.youtube.com/watch?v=6cXXsYBwrHQ***

# 6. Digital Health and Wellness

### *6.1 What is digital health and wellness?*

Digital health and wellness is the ability to use technology like mobile phones, laptops, desktops and tablets and not use it too much to the point of hurting your mind or your body. Excessive and improper use of technology could cause lifestyle problems that will affect your everyday life and ability to do things. You may develop physical ailments like back problems and carpal tunnel or psychological disorders.

## Golden rules

*- Avoid excess of anything, including the time spent online. Set screen time.*
*- Use technology with a positive attitude and follow good practices to safeguard your devices and their usage, and your personal security.*
*- Do not eat and surf the net at the same time.*
*- Seek help if you are neglecting your routine activities, such as personal hygiene, food and water, time spent with your family and friends, physical activities and offline hobbies.*

### *6.2 Opportunities and risks*

Mild use of digital technology tends to be beneficial for children's mental well-being, while too much use may have a negative impact. Be aware of the inherent dangers of digital technologies, consequences of excessive use (e.g., eye safety and repetitive stress syndrome), and psycho-social issues that are becoming increasingly prevalent.

**Physical health problems and obesity:** As time spent on digital technology increases, time spent on physical activity is reduced, which might be a contributing factor to child and adolescent physical health problems. The time spent on digital technology does, to some extent, take time away from other activities, which in some situations (such as periods of high volume of school work) can be problematic. Lack of physical activity can be detrimental for health and well-being.

**Limited movement of limbs:** When people spend countless hours daily hunched over numerous types of handheld devices with their heads bent forward, they are at risk of developing "text neck." Complaints associated with text neck are neck, back, arm, finger, hand, wrist and elbow pain, as well as headaches and numbness and tingling of the upper extremities. There is a chance of developing shoulder complaints.

**Eye strain:** Eye redness or irritation from staring at the bright backlight of screens for long periods, dry eyes due to reduced blinking, blurred vision and general fatigue from staring at screens and straining to see small fonts and images are all symptoms of digital eye strain. If you use a number of devices simultaneously, the chances of eye strain increases. Headaches may occur from repeated eye strain.

**Hearing loss:** Prolonged exposure to high volume sounds, especially with ear plugs and phones, can contribute to hearing impairment. You can keep your hearing intact by following the 60/60 rule.

## 60/60 rule

*Listen to any device at a maximum of only 60 percent of its full volume for a total of 60 minutes a day. By taking this advice as an early warning, we can protect the hearing that we have now, and carry on enjoying the wonders that sound brings to life.*

**Accidents:** Avoid use of online activities like selfie, social media use or any other online activities to avoid accidents while you are on the move. Traffic rules also have made this a punishable offence and invite fines.

Do not take unnecessary risks in trying to get the perfect and unusual selfie for posting. There have been several accidents and persons have lost their lives. While it is good fun to get good pictures to capture the moment, do not allow the social media obsession for the 'perfect' selfie, or the number of likes you get, influence your judgement or affect your self-esteem or force yourself to compare yourself with others. Be proud of your own unique personality and abilities. Being good in practice is better than being preoccupied with looking good in pictures.

**Selfies: A Boon or Bane?**

*A study by researchers at the All India Institute of Medical Sciences (AIIMS) in 2018 noted found that about half of the 259 reported selfie deaths and accidents between 2011 and 2017 occurred in India. People below the age of 30 in India was the group often killed while taking a selfie. Behind India, other countries with the most selfie-related deaths included Russia, the United States and Pakistan.*

*The majority of the so-called "killfies" the researchers identified were caused by drowning, being hit by a train or car, or falling from a great height. But they said the total number of deaths could actually be much higher, as many cases go unreported and "death by selfie" is not recognised as an official cause of death.*

*The study did not include near-misses, such as the case of one Indian man who survived being struck by a train while taking a selfie in January 2018. Nor did it include the 48 people who reportedly suffered burns while taking selfies in front of a bakery ablaze in 2017, ignoring police demands that they stop snapping images.*

***Abuse and addiction:*** Excessive use may not be addiction. If the user is using digital technologies for genuine purposes, e.g., home work, research, essential communication and moderate leisure, and does not hamper other routine activities, the time spent online may be justified.

The following pointers may help you in understanding your own use of digital devices and the internet and set time limits before parents, teachers or counsellors need to intervene.

WATCH

*https://www.youtube.com/watch?v=4dsFKIY-tYw*

**Evaluate your own online use by asking these questions:**

- *Do you check the phone first thing upon waking in the morning?*
- *Do you check your phone frequently throughout each day?*
- *Do you have a hard time unplugging at night?*
- *Do you look at the phone while in conversation with friends or family?*
- *Do you picking up the phone whenever you are bored?*
- *When offline, are you preoccupied with getting back online?*
- *Do you forget doing homework or other household tasks for being on the Internet?*
- *Have you lost all interest in the activities you used to enjoy and spend a lot of time online?*
- *Are your online activities stopping you from spending time with friends and family?*
- *Do you prefer being online than being around real, live friends and family?*
- *Do you seek new friendships with people met on the Web?*
- *Does the number of friends, likes and views on social media affect you?*
- *Is your academic performance in school getting affected?*
- *Are you learning something related to your goals in life through your online activities?*
- *Is your online time contributing to your school assignments, career goals, and entertainment?*
- *Is your online time contributing to your hobbies or special interests?*

*By answering these questions you should consider whether you need to be conscious you are getting too absorbed in the technology and it is affecting your normal activities, relationships and life and career goals and you need to regulate your online time and activities.*

Discussion and negotiation with adults, e.g., parents, guardians and teachers, do help in identifying if the quantum of use is excessive. But over a period of time, increasingly excessive use of digital technologies can lead to addiction.

**Nomophobia**

*"No Mobile Phone Phobia", is the irrational fear of being without your mobile phone or being unable to use your phone and the services that the phone provides (especially phone calls and Internet connection) for some reason, such as the absence of a signal or running out of minutes or battery power. A phobia is by definition an irrational fear."*

The WHO has recognised "gaming disorder" or a "pattern of persistent or recurrent gaming behaviour" in which people lose control of their gaming behaviour, give priority to gaming over other interests and activities, and continue gaming despite negative consequences, such as impairments in their family relationships, social lives, studies or work or other areas as a mental health condition. It has added it to the International Classification of Diseases. But simply playing a lot of video games is not enough to count as a disorder. It is important to identify the stages of experimentation, use and abuse before addiction sets in.

It is a good idea to consult a trained and qualified psychologist or psychiatrist. who have the knowledge and tools to determine if indeed you have addiction and help you overcome it. They will assess if the duration of time spent on using the digital device or platform is affecting behaviour, if the technology is being used for rightful purposes and is not causing neglect of other aspects of life, and if the behavioural pattern is negative and causing significant mental health issues (e.g., irritation, short attention span, low self-esteem and self-harm). Preoccupation or the desire to continuously use digital devices and the internet, the loss of control while using them and experiencing consequences due to use together in your lifestyle for the last 12 months, or in some cases may even be in the last three to six months, can indicate addiction.

***Real versus virtual life.*** Appreciate the distinction between real life and virtual life. Our "virtual life" is just a part of something greater: our real life. One of the main causes of nomophobia is the idea of giving a "virtual-life experience a status, which may be equal or even greater than what we experienced in our "real" life. One needs to disconnect from the 'constructed' identities we all feel we need to develop online and have the confidence of being who one really is.

How many "likes" and "shares" a social media post receives is not an indicator of popularity, or personal worth, which should influence self-esteem. The "fear of missing out" or FOMO can be a strong driver, especially when others in school or friends circle share images on social networks and can create a strong pull to be part of the 'in' crowd. The principle of YOLO or "you only live once" reinforces the hedonistic idea that the one life one has is meant to be enjoyed. But there is a very fine line between trying new things and endangering yourself. With new online challenges and trends coming up every day, make sure you keep in mind your safety first.

Passive browsing of social networking sites can also make children envious of other people's online personas, real or carefully crafted, potentially leading to feelings of inadequacy. As they say - the grass is greener on the other side of the fence. Cultivate personal interests and hobbies offline, meet friends offline and spend time with the family as they can add value to your life.

Cyberbullying is known to cause depression, social anxiety, and diminished quality of family and social relationships. It may also lower academic performance and push the victim to risky behaviour. It can be prevented with some help, motivation and courage.

Cyberstalking causes stress, anxiety disorders, fear and psychological trauma regardless of the fact whether the victim actually meets the harasser or not and experiences a feeling of helplessness and maybe lack of support.Change in eating and sleeping patterns may also be observed.It is advisable to immediately inform a trusted adult if such an incident occurs and seek help and not keep quiet about it.

## *6.3 Good practices*

### *6.3.1 Everything in moderation*

Excess of anything is harmful. If used judiciously, without disregarding other essential aspects of life, the benefits of digital technologies can be harnessed, and with great effect. Balance the time spent on online modality/ with other uses, for example, school assignments, social interactions and outdoor activities. Balance time spent on using technology devices with physical activity as well as interpersonal interactions in daily routine.

***Time limit for the use of digital devices.*** Setting limits for the time spent with mobiles, laptops, desktops and tablets enables the user to do other important things and lead a balanced and fulfilling life.

However, it is difficult to say how much is too much. You can show responsible use of your time and good judgement by regulating and balancing your time use sensibly.

Put a limit on the information that you receive. It will help you process and use the information you already have, and identify what more information you need to acquire. Frequently, messaging applications offer you the option to remove the features that can create so much anxiety. Use them, you do not need to spend all day wondering about what someone else is doing.

***Setting screen time.*** Are you in the habit of constantly checking notifications? Do you constantly wonder whether your contacts have read your messages?

### *6.3.2 Periodic digital detox*

Find certain moments to disconnect yourself from a mobile phone. Switching off while having meals and sleeping, and setting other "no mobile" or "silent mobile" time slots are not only good but necessary. Place your phone at least 15 feet away from you when you sleep at night. Keep it silent and resist the temptation to check it before the morning. Turn off the mobile phone while having conversations and interactions with people.

Aerobic exercise will help to sustain strength, improve cardiovascular conditioning, and counteract the strain of sedentary computer use.

### *6.3.3 Sound ergonomic practices*

Simple ways can prevent possible harms resulting from the continuous use of mobile phones, laptops, desktops and tablets.

Alternate tasks to make changes in your working position to avoid making the same movements for prolonged periods of time. Prolonged use of a computer keyboard and/or mouse can cause muscle aches and nerve pain. Customize your computer to maximise comfort and efficiency by using your software. Adjust the screen font, contrast, pointer size, speed, and colour of the digital devices.

#### (a) Posture

Maintain good posture when working at the keyboard. Sitting on a chair with back support is helpful.

**Neck and trunk:** Avoid twisting or bending them. Avoid excessive reaching. Position frequently used items directly in front of you and angled upward on a copyholder when working.

**Shoulders:** Keep your shoulders relaxed with your elbows close to your sides.

**Feet:** Keep your feet supported on the floor or on a footrest when you work to reduce pressure on your lower back

**Elbows:** Avoid resting your elbows on the hard surface or edge of your table. Use pads to protect your elbows if necessary. Elbows positioned at 100 to 110 degrees when working help with a relaxed position at the keyboard. Elbows should be positioned at 100 to 110 degrees when working in order to keep a relaxed position at the keyboard. This could require a slight negative tilt (front of keyboard higher than back) when working in upright positions. If reclined in your chair, the keyboard could be at a positive angle to maintain this relaxed position.

**Wrists:** Your wrists should be in a neutral or straight position when keying or using a pointing device or calculator. Wrist rests can assist you in maintaining a neutral position when used properly during pauses. Float your arms above the keyboard and wrist rest when keying. Avoid planting your wrists on the table or wrist rest. This can result in bending the wrists either up and down or side to side.

**Hands:** Your hand should be relaxed. Keep your fingers and knuckles relaxed when working at the keyboard. Avoid holding your pointing device tightly. Never hold a pen or pencil in your hand when keying. Avoid hitting the keyboard with excessive force. Studies have shown that the average user hits the keyboard with four times the required force when keying.

**Eyes:** Blink your eyes frequently while focusing on the screen. Rest your eyes by refocusing on distant objects intermittently when working. Take a one or two-minute break every 15 to 20 minutes, or a five-minute break every hour to stretch your limbs. Every few hours, get up, move around, and do an alternative activity.

**(b) Positioning**

a) When writing at the computer, avoid excessive reaching over the keyboard or work materials. Your keyboard, pointing device, files and telephone should be within easy reach. A sturdy in-line copyholder can double as a writing surface if appropriately positioned.

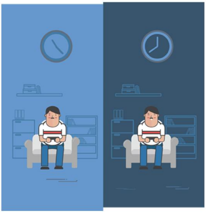
b) Use a keyboard tray to properly position your keyboard and pointing device.

c) Use a copyholder positioned in line with your monitor and keyboard.

d) Position the monitor so that the viewed part of the screen allows you to keep your neck in a neutral or straight position. The monitor should be centred directly in front of you. The top of the computer screen should be slightly below the top of your head, so that you are looking at it with a slightly downward gaze.

e) Position your monitor to eliminate excessive glare or reflections from windows and lighting.

*https://www.ehs.pitt.edu/workplace/ergo-tips.html*



You can also reduce strain by using features like swiftkey which will help you type faster and more easily by simply sliding your finger on you phone keyboard. You can also use the option of "Sticky keys" on PCs to create shortcuts and make your work easier.

**Use only the apps that you really need.**

a) Installing an endless number of apps (especially social networks) on your mobile phone can be a total trap. While communication options multiply, a person suffering from nomophobia needs to feed their addiction even more. Therefore, not installing that many applications can be a good way to avoid the temptation.

b) In order to feel liberated, try a technology fast every month where you actually go for a day or more without a computer, tablet or phone.

Technology should improve lives and not enslave the users. That is why, using technology in a reasonable way will always be the smart choice. And if you are not able to do it by yourself, do not hesitate to ask for help.

***6.4 Sharing problems to seek solutions***

Talking about the problem can be the first step to solving it. If something upsets you online or you are worried about a friend it can really help to talk to someone. There are lots of people who can help you, such as friends, family members and teachers. Talk to an adult who you trust. Talking about a problem can often make you feel better. If you keep your worries to yourself they can grow. It is a lot easier to solve a problem when there are two heads working together on it.

Often we do not talk to our friends or parents about the things we would like to because we feel embarrassed, shy or ashamed. The thing to remember is that whatever it is you are embarrassed about; a good friend is not going to laugh at you or put you down. They will listen, try to understand and try to help you feel better or find a solution. And that's why people find that talking to a good friend about a problem usually does help.

The services that you use online should also offer a reporting service, such as being able to talk to a moderator or report other players. It is important that you talk to an adult you trust if anything has upset you or made you feel uncomfortable whilst online. Remember you can always call ChildLine on 1098.

**Peers.** Communicate with your trusted friends, especially those who know more about the problems or have had similar experiences, without the fear of being judged. However, a certain level of knowledge and sensitivity is required for solutions so do approach an adult who has your trust for advice and support.

**Parents:** Speak with and seek help from parents if some kind of "family agreement" has been arrived at through dialogue within the family.

***Open discussions and family agreements***

*Although the risk of abuse online is clearly serious, the capacity of most children (and their parents) to protect themselves is often under-estimated. Open and informed discussions among parents and children about the internet from an early stage can be the best defence against online grooming and bullying.*

*Parents often seek the security of their children but they should not be snooping, which can leave children feeling untrusted and increase the risk of self-harm. Ideally, a family agreement is a good way to start a conversation with the whole family about how everyone will use the internet and discuss together how to behave in a positive way when online at home, at school or at a friends house.*

**School counsellors or teachers:** If your school has a counsellor, discuss your problem you with them. They are there to answer your questions and provide guidance and assistance. You may even approach a teacher or school staff who you trust and feel comfortable speaking with.

**Seeking help from experts.** Professional expertise is available, although not everywhere, to assist with various problems related with misuse or excessive use of digital devices and technologies.

The following institutions are well-known for their expertise on digital health and wellness.

a) SHUT clinic (Service for Healthy Use of Technology), National Institute of Mental Health and Neurosciences (NIM-HANS), Bengaluru, Karnataka

b) Department of Psychiatry, the All India Institute of Medical Sciences, New Delhi

WATCH

*https://www.youtube.com/watch?v=kvgJIFn_e04*

# 7. Digital Rights, Freedoms and Responsibilities

### *7.1 What are digital rights?*

Digital rights are basically human rights in the digital era, when internet is increasingly being regarded as a right rather than a luxury. The rights to online privacy and freedom of expression, for example, are really extensions of the equal and inalienable rights laid out in the United Nations Universal Declaration of Human Rights. According to the United Nations, disconnecting people from the internet violates these rights and goes against international law.

Digital rights include access and participation, free speech, community, privacy, physical and psychological safety, safety of identity and of material and intellectual property. But as Uncle Ben said in the Spider Man, "with great power comes great responsibility." The responsibilities include knowing and respecting the community standards and guidelines of all social media, video platforms and online groups being used and staying within the parameters of these guidelines.

If any activity is in violation of the community guidelines set by a platform, it may result in the post/comment/photo/video/account being deleted.

***Snapchat Community Guidelines : https://www.snap.com/en-US/community-guidelines***
***Instagram Community Guidelines: https://help.instagram.com/477434105621119***
***Facebook Community Guidelines: https://www.facebook.com/communitystandards/***
***WhatsApp Community Guidelines: https://www.whatsapp.com/legal/***
***Twitter Community Guidelines: https://help.twitter.com/en/rules-and-policies#general-policies***

| *Right in the CRC (Offline)* | *Issues arising from the digital age /evidence* | *Internet Rights and principles (protect children's rights) (Online)* |
|---|---|---|
| PROTECTION:<br><br>From all kinds of discrimination (Art. 2) from information and materials injurious to the child's wellbeing (Art.17e) arbitrary or unlawful interference with his or her privacy, family or correspondence and unlawful attacks on his or her honour and reputation (Art.16) against all forms of abuse and neglect (Art. 19), including sexual exploitation and sexual abuse (Art. 34), and other forms of exploitation prejudicial to child's welfare (Art. 36) | • Differential access to technology by gender, rural/urban and geographic area, language, disability, etc.<br>• Sexual grooming and exploitation<br>• Creation and distribution of child abuse images<br>• Online dimension of trafficking<br>• Strangers repeatedly contacting<br>• Exposure to violence<br>• Threats to privacy, identity<br>• Exposure to diverse and extreme pornography<br>• Personal data exploitation or misuse, including location based and financial data<br>• Cyberbullying content and conduct, hostility, hate<br>• Reputational risks<br>• Blackmail/exhortation<br>• Persuasion - suicide, self-harm, pro-anorexia, drugs | • Dignity must be respected, protected and fulfilled online<br>• Privacy, freedom from surveillance and censorship and right to online anonymity to be safeguarded<br>• Control over personal data collection, retention, processing, disposal and disclosure<br>• Protection against harassment, hate, defamation, crime and sexual exploitation<br>• Children should be free to use the internet and protected from its risks and threats based on evolving capacities |

| *Right in the CRC (Offline)* | *Issues arising from the digital age /evidence* | *Internet Rights and principles (protect children's rights) (Online)* |
|---|---|---|
| **PROVISION:**<br><br>to support children's right to life and development (Art. 6)<br>to preserve his or her identity (Art.8) to education to support development of his or her full potential (Art.28) and prepare them for a responsible role in a free society (Art.29) to recreation and leisure appropriate to their age (Art.31)<br>to diverse material of social and cultural benefit to the child (including minorities) to promote children's well-being (Art. 17) to all measures for recovery from neglect, exploitation and abuse (Art. 39) | • Formal and informal learning resources and curriculum<br>• Wealth of accessible and specialised information<br>• Opportunities for creativity exploration and expression<br>• Digital skills and literacy<br>• Ways to counter inequalities<br>• Expanded entertainment choices<br>• Access to cultural and heritage content online in an equitable way | • Life, liberty and security<br>• Access and use of a secure and open internet, including addressing special needs of disabled children<br>• Cultural and linguistic diversity on the internet must be promoted and innovation should be encouraged to facilitate plurality of expression<br>• Education through the internet, to culture and knowledge online |
| **PARTICIPATION:**<br><br>In all actions concerning children... the best interests of the child shall be a primary consideration (Art. 3), including the right of children to be consulted in all matters affecting them (Art. 12);<br><br>see also child's freedom of expression (Art. 13)<br>and freedom of association and assembly (Art.14)<br>to information (Art.17)<br>and to participate fully in cultural life (Art.31) | • Enhanced networking opportunities<br>• Ways of consulting children in diverse situations and processes including consulting them on education, research and online issues<br>• Platform for children's voices Child-led initiatives for local and global exchange<br>• Peer to peer connections for sharing and collaboration<br>• Recognition of rights and responsibilities | • The internet is a space for promotion, protection and fulfilment of human rights and advancing social justice, including for all children<br>• Seek, receive and impart information freely and to associate freely with others for social, political and cultural purposes |

CRC- Convention on the Rights of the Child, ratified by the Government of India in 1992

Table adapted from UNICEF and Child Rights in the Digital Age by Sonia Livingstone

The UN Committee on the Rights of the Child is in the process of finalising a General Comment on Children's Rights in relation to the Digital Environment, which will provide global guidance to all countries on how different stakeholders can take measures to protect children's rights.This will become available shortly on the following website:

***https://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx***

***Golden rules***

- *A right is the right thing to do. Every right comes with a corresponding responsibility.*
- *Use technology in a manner that respects the rights of others, including the right to privacy and free speech.*
- *Act within the law, follow the norms of decency, and pose no serious risk of harm to yourself and others.*
- *Do not breach the community standards. If you do, the service provider or administrator may intervene to take corrective measures, which can affect your digital footprints.*
- *Read the fine print when you first use an online service.*

### *7.2 The right to education and access to information*

All children have a right of access to digital technologies. No child should be deprived of this right on any grounds, be it gender, age or socio-economic status. In this digital age, they have the most to gain from these technologies, and also the most to lose from remaining cut off. The government has a legal duty to ensure that children have an education, and can access information widely and equitably in support of their development and well-being. Children's right to free expression also requires that they be able to seek out information and ideas of all kinds.

Except where limiting access to content is clearly required by law, and that law meets the children's rights standards set out above, educating children in digital literacy is a preferable means of safeguarding them from harm.

### *7.3 The right to privacy*

The right to privacy recognises children's authority over their personal information. Asking children for their consent to collect their information shows the greatest respect for children's right to privacy. Consent must be free and informed and a child must be able to withdraw at any time. If a child does not have the capacity to consent, then their consent can never justify the collection of their information.

Children are especially vulnerable to exploitation of their personal information by both commercial and state agencies, whose data-harvesting practices remain largely unregulated in most parts of the world. Children are less likely than adults to be aware that they have a legal right to privacy, that their online activity is automatically recorded, and that they are targets for organisations collecting their personal data for commercial gain.

***Do you click "agree" without reading the terms of service of internet companies? Be careful or with your tick of acceptance, you may be forfeiting your data and the right of redressal.***

Efforts are being made by the government to have in place measures to prevent, manage and raise awareness of reputational risks, privacy intrusions, cyberbullying, pornography, personal data misuse (including identification of location-based and financial information).

***The right to be forgotten***

*The right to have data about oneself erased or withdrawn by service providers is the right to erase the past unwanted history of a user by the social media and search engines, is an evolving concept which is being discussed in several fora. There is no explicit provision covering this at present except for its explicit recognition in the European Union's General Data Protection Regulation (GDPR), which upholds the privacy of citizen data and makes it difficult for the companies to use it for commercial purposes without the consent of users. While legal experts are advocating the right to be forgotten strongly in the context of privacy rights, it would take quite some time before an agreement is reached globally on its scope and modalities.*

Parents, schools and the state are usual suspects when monitoring and surveillance of children's physical whereabouts and online activity are discussed. Monitoring technology ranges from apps for parents that report their child's whereabouts to the screening of schools for potential criminals using IT systems that collect information about children's activities.  For example, many online services, such as games, require children to provide detailed personal information as a condition of access, such as by logging in using their Facebook credentials. Once access is granted, providers track online activity in detail, and may persuade or lure children to disclose further personal data using personality questionnaires and similar tactics. Often, the sole safeguard against this is a privacy policy or statement of terms of service, which is typically a routine requirement and most often written in not too transparent a language.

Monitoring is by nature intrusive, and does not ask for the consent of children and young people. When they are not even informed, it can be counter-productive. Open discussion on monitoring of children's use of technology may foster mutual trust, and awareness could lead to positive digital communication and safe online conduct.

However, the monitoring by parents and caregivers in deciding the scope and nature of the information and content that younger children access may be considered more positive, if but this gives way as children mature and their capacities evolve to make these decisions for themselves. This is the reason why one must be aware of all steps in safeguarding personal data while browsing the web, using social media, gaming, and engaging in other activities online.

## *7.4 The right to be safeguarded from violence, abuse and exploitation*

Children have a legal right in international and most domestic law to be safeguarded from abuse, including sexual abuse. The legal responsibility is on the government to prevent abusers from contacting children.  The government needs to take all measures to make the internet as safe as possible an environment through measures to prevent the creation and distribution of online child abuse imagery, sexual grooming, and online dimension of child trafficking. Children need to be made aware of how to prevent online abuse, and if need be to know where to report and seek help.

**Case 1**
A class 7th school girl from UP was sitting outside her house in a rural area and washing some utensils. The boys who lived in the neighbouring house took photos of her body that was visible because she was squatting. They then blackmailed her and asked her family to leave the locality immediately, or they would find the photos all over the internet. The girl opened up after weeks of torment. She finally filed a complaint and the boys were apprehended and warned by the police. And she has never been bothered since then.

Lesson: Do not hesitate to open up to parents or police officials. Not telling and suffering in silence is the worst thing one can do to oneself. Be courageous and bold and share your problem with the trusted people.

***Case 2***

An impersonated account was created in the name of a young girl studying in class 10th.The photos of her and members of her family were morphed, and their mobile number shared on the impersonated Facebook profile. She received a lot of obscene phone calls, and was terrified. She finally talked about the problem with authorities. A formal complaint was filed. The offender was identified and penalised.

Lesson: Do not hesitate to seek help from parents, friends or any adult that you trust. Report as soon as you find any suspicious account using your names or photos.

Case 3

A young girl of class 6th was taken by her uncle to his workplace, a clinic. They played hide and seek and then the uncle offered a glass of juice to the girl. She drank the juice and fell unconscious. When the girl woke up she felt uncomfortable and her body hurt. She hesitated to share this with her family as she went along with a relative trusted by the family. After a month, she opened up about the incident and spoke to her school teachers. They in turn spoke to her family and action was taken against the uncle by authorities.

Lesson: It is always advised to share the problems with your parents. Even if the offender is from family itself, do not sit back and think whether to report or not. It is always safe to share with the parents.

***Source: Experiences narrated by children and young people to CPF***

## *7.5 The right to freedom of expression and the right to be heard*

Children have a right to freedom of expression, and also a right to have their views heard in all matters affecting them. As a legal principle, the right of freedom of expression is more important than the policy preferences of schools and other institutions. Any restrictions on this fundamental freedom are not legitimate unless required by law and strictly necessary to safeguard the rights of others, national security, public order and health. It is the responsibility of the government, the internet industry and society at large to protect the internet as a space where children can express themselves without undue anxiety, and to safeguard their right to be heard in their own interests. Children should not attract suspicion for exercising these rights.

## *7.6 Children's rights to leisure and age appropriate recreation*

Children have a right to recreation and leisure as appropriate to their age, an education that will support the development of their full potential and prepare them for responsible life in a free society. To ensure this right, the government and educational authorities have to take measures to provide educational technology, online information and creative resources and promote digital skills equitably, factoring in differences in languages, access or conditions of disability or disadvantage.

## *7.7 Children's right to participation*

The Convention on the Rights of the Child states that "In all actions concerning children… the best interests of the child shall be a primary consideration". This right includes the right of children to be consulted in all matters affecting them, which is seen in conjunction with the child's freedom of expression, and freedom of association. The government and its agencies, service providers, educationists and school administrations and civil society organisations are expected to provide children and young people for their inclusion in diverse societal processes, including consulting them on matters related to their education, research and ICT governance when it affects them.

**Have you ever participated in any discussions in your family and school about responsible use of digital devices and internet?**

### *7.8 The right of access to redress and justice*

Children have a right to justice. Ensure that children have avenues for formal, including legal complaint in cases where their online rights have been breached and the support to make effective use of these complaints procedures. Children have to be made aware of all these provisions and how to use them if required. They also need to know who to go to for guidance and support.

### *7.9 The right to intellectual property*

In principle, children have the right to intellectual property. The Indian Contract Act prevents minors from entering into a contract but permits the claim of intellectual property rights for their original creations through the legal process of claiming copyright. The practical and legal difficulties surface while dealing with the question of who should enjoy the economic benefits of copyright surfaces and requires solution of the problem regarding who should enter the contract with whom.

Most social media websites, including YouTube allow children above the age of 13 to register. However, parental guidance and monitoring is a must because the norms and policies of websites need to be vetted carefully.

WATCH

***https://www.youtube.com/watch?v=bXYi-b6tiV8***

# 8. Digital security

### *8.1 What is digital security?*

Digital security is an all-encompassing term, which includes the tools to secure technology, assets and personal identity in the online and mobile world. Good practices and tools such as anti-virus software, web-services, biometrics and secure personal devices, e.g., smart-card based USB token, the SIM card, the secure chip in payment card or an ePassport are digital security devices because they offer freedom to communicate, work, travel and shop using your digital identity in a way that is convenient, enjoyable and secure.

### *8.2 Security of devices*

Smartphones, laptops and tablets are all open to wireless security risks. Protect them against cyberattacks.

#### *8.2.1 Common threats to devices*

Viruses on digital devices are malicious programme codes that can corrupt the system and destroy the data within the computer.

- ***Malware*** is a type of malicious software designed to gain unauthorized access or to cause damage to a computer without the knowledge of the owner. Malicious files or programmes, such as worms, computer viruses, Trojan horses and spyware, can steal, encrypt or delete sensitive data, alter or hijack core computing functions and monitor users' computer activity without their permission.

- ***Ransomware*** is a type of malicious software designed to extort money from the user. The attacker locks the victim's computer system files or blocks access to files or the computer system typically through encryption until the ransom is paid. Paying the ransom is no guarantee that the files will be recovered or the system will be restored. While this has declined in recent times, it still remains as a serious threat.

Several public locations like cyber cafes, shopping malls, airports among others offer their customers free access to public Wi-Fi. The service is very convenient for checking messages and attending to urgent tasks.

But public Wi-Fi networks also enable cyber criminals to spy on unwary customers and intercept their data that is transferred across the link. They can access sensitive information of users' banking credentials, account passwords and other valuable information. Many mobile and laptop users risk the security of their personal information, digital identity and money. The risks are even greater if the devices are not protected by an effective security and anti-malware product.

A hacker is someone who uses or exploits technology for an unintended use thereby disrupting operations or causing financial or reputation loss to people. Hackers often use malwares, viruses or Trojans to attack computer and gain access to your data.

Hacking is a broad term used to define gaining entry into a computer without permission, with the intention to harm, cause loss, steal, or destroy the data contained in it. Usually hackers are well versed with computer technologies by using various applications or programmes that penetrate the defence mechanism employed by the target computer and send back the sensitive information like usernames, passwords, IP addresses and using them to gain access into the computer itself. These applications or programmes can be in the form of Trojans, worms, malware and viruses, which will install in the system and compromise its security. After all of this the hacker can gain administrative rights and can do anything with the data contained in the compromised computer system.

#### *8.2.2 Preventing and countering threats and risks*

**Install anti-virus software.**

Make sure all of your devices are protected by a rigorous anti-malware and security solution — and ensure that it's updated as regularly as possible.

***a) Regularly update software and operating systems.*** Exploiting email and web browsing applications is the most common way hackers and malware try to gain access to devices and your information. Protect yourself before you start browsing the web by making sure that your operating system, web browser, security software, browser plugins (like Java or Adobe products) and other applications are up-to-date.

***b) Use privacy settings on mobile phones, apps and browsers.*** Privacy settings on social media platforms enable you to select who can access your posts online. Try to restrict access of your profile to your friends only. Remember what you post online remains there almost forever, so do not post personal phone and other details on social media platforms.

***c) Verify if the Wi-Fi link is legitimate and safe.*** Treat all Wi-Fi links with suspicion. Public Wi-Fi is inherently insecure — so be cautious. The Wi-Fi link could also be a bogus link set up by a cybercriminal trying to capture valuable, personal information from unsuspecting users. Don't connect to an unknown or unrecognised wireless access point. Try to use known Wi-Fi links, which are password protected.

- *Try to verify it is a legitimate wireless connection*
  *Some bogus links set up by malicious users — will have a connection name that's deliberately similar to the facilities offering free Wi-Fi. Verify before using.*

***d) Learn to create VPN to avoid downloading of data through public Wi-Fi.*** Use your mobile phone to create VPN* If you need to access any websites that store or require the input of any sensitive information consider accessing them via your mobile phone network, instead of the public Wi-Fi connection.

**VPN or Virtual Private Network helps you connect to the internet in a safer and more secure way.*

***e) Verify if the website is legitimate/authentic.*** Avoid logging into websites where there's a chance that your identity, passwords or personal information may be compromised from public facilities— such as social networking sites, online banking services or any websites that store your credit card information. (How to check authenticity of websites, chapter)

***f) Download apps from trusted sources like Google play, AppStore***

***g) Keep webcams private.*** These devices can sometimes be hacked and used to take pictures or videos of you without your consent. Put a sticker over your webcam, laptop camera, or phone camera when they are not in use.

***h) USB Storage Device Use***

- Always delete the device clearly to clear the content
- Always scan the USB device with latest antivirus before accessing
- Protect your USB device with a password
- Encrypt the files/folders stored on the device
- Use USB security products to access or copy data on your USB
- Do not accept a promotional USB from unknown persons
- Do not keep sensitive information like username and passwords on the USB

***g) Disable Bluetooth and Airdrop when not in use***

Monitor your Bluetooth connectivity. Bluetooth is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can compromise cybersecurity. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, school, or similar secured area.

**AirDrop** feature allows you to send any kind of content like photos, videos, documents from one Apple device to another wirelessly. It doesn't impose any restrictions or limits on the file size. AirDrop makes use of the Bluetooth technology to detect and pair with other Apple devices which are located within the range of Wi-Fi and Bluetooth. It is highly recommended to turn ON AirDrop only during file transfer.

**At all other times, turn off that feature to avoid receiving files from unknown contacts.** When you are not sending files to someone, then you can turn off the AirDrop either from the **Control Center** or from the **Settings** menu. If not needed, you can also turn off Bluetooth to save your iPhone battery

## *8.3 Operational security*

### *8.3.1 Passwords*

Strong, unique but easy to remember, and private passwords are essential for dealing with unauthorised access to online accounts. The passwords, when shared with other person(s), can be misused. They may be stolen by unauthorized users to collect and misuse your personal information.

Learn how to create strong passwords and passphrases. A password must be difficult to guess. But you should be able to remember it. Writing passwords somewhere is not advisable. Memorise it. Your password is given to you to maintain your privacy.

| *Strong* | *Unique* | *Secret* |
|---|---|---|
| *Use at least 8 characters or more to create a password. The more number of characters one uses, the more secure is the password.*<br><br>*Use various combinations of characters. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters.* | *Avoid using the words from the dictionary as they can be cracked easily. Do not use the name of things located around you. Do not use a password that was used earlier.*<br><br>*Do not use a password that uses your personal information like nicknames, phone numbers, date of birth etc.* | *Do not share passwords with anyone, not even your friends.*<br><br>*Be careful while entering a password when someone is sitting beside you.*<br><br>*Change the password periodically or when you suspect someone to know the password.* |

Go for an extra layer of security by opting for two-factor authentication (2FA), also known as two-step verification or dual factor authentication. This security process requires the user to provide two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

Log out of your account when you plan to be inactive even for a short while. Always keep your system locked whenever it is not in use.

### *8.3.2 Emails and messages*

Most email providers offer filtering services.
The use of Rich Text Format instead of the standard .DOC format will retain the formatting but not any macros. This may prevent you from sending virus to others if you are already infected by it.

| DO | DO NOT |
|---|---|
| • Use email filtering software to avoid spam so that only messages from authorized users are received.<br><br>• Scan the attachment with received messages with updated antivirus software before saving it.<br><br>• Be very careful while downloading attachments from emails into your hard disk. | • Send personal information through emails.<br>• Click on the emails received from untrusted users and the links that come via email.The act of clicking may execute some malicious code and spread into your system.<br>• Open attachments with emails from strangers. They may contain a virus along with the message.<br>• Send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files.<br>• Fill forms that come via email asking for your personal information. |

### *8.3.3 Security settings on the browser*

- Update anti-virus software regularly.

- Adjust the settings in the web-browser. It may limit some functionality but can provide the best protection from malicious content.

- Enable email accounts for multi-factor authentication. Email is the gateway to almost every other account a user may have. When someone loses or forgets an account password, the reset is sent to his or her email.

- Gauge the credibility of the website by checking the url, lock,

- Look out for warning signals given by web browsers about exposure to a malicious website or content. Such warnings can protect the user from malware, phishing and identity theft. These warnings given by most of the commonly used browsers like Chrome, Internet Explorer, etc. Remember to update your browsers regularly to avoid missing out on such updates.

- Exercise caution while giving details about personal information when registering for access to email accounts, social networks and chat rooms, and free game downloads.

**Data accessibility and privacy**

Certain online activities compromise the privacy of children.

**Filling online forms for surveys, contests, downloading games on commercial or free websites.** Some websites prompt the users fill-up their form for participating in games, surveys and contests. The name, email id, age and gender, and at times the telephone number and postal address, obtained in this manner can be used to access information.
Some requests are legitimate: much depends on the nature of the website requesting the information. Providing personal information online can result in a student being targeted for spam (unsolicited email), advertising materials and/or virus-es.

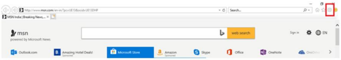
Privacy issues also apply to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illicit purposes.

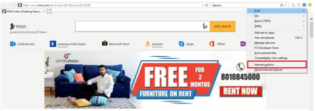
**A screen lock (or lock screen)** on the mobile phones and computers helps to prevent unauthorized access. In order to use a lock screen protective device, a specific action or sequence of actions has to be performed correctly. It could be the entry of a password or passphrase, a specific gesture or motion on the touchscreen, or fingerprint on the biometric reader, scan of eyes or other facial features for recognition of the authorised user.

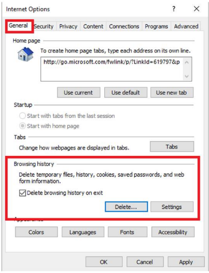
Use the following advice when browsing the web to reduce your risk of being a victim of cybercrime:

Settings and security models are different for each browser. Visit the following vendor websites to learn more about the security settings in your browser:

**INTERNET EXPLORER**






Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Home page

To create home page tabs, type each address on its own line.

http://go.microsoft.com/fwlink/p/?LinkId=619797&p

Use current | Use default | Use new tab

Startup

Start with tabs from the last session

Start with home page

Tabs

Change how webpages are displayed in tabs. | Tabs

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

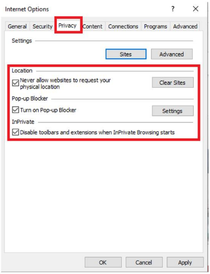
☑ Delete browsing history on exit

Delete... | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply


Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Sites | Advanced

Location

☑ Never allow websites to request your physical location | Clear Sites

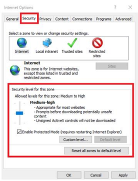
Pop-up Blocker

☑ Turn on Pop-up Blocker | Settings

InPrivate

☑ Disable toolbars and extensions when InPrivate Browsing starts

OK | Cancel | Apply


Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

**Internet**

This zone is for Internet websites, except those listed in trusted and restricted zones. | Sites

Security level for this zone

Allowed levels for this zone: Medium to High

**Medium-high**

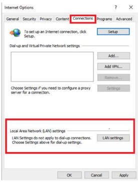
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply


Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

To set up an Internet connection, click Setup. | Setup

Dial-up and Virtual Private Network settings

Add... | Add VPN... | Remove...

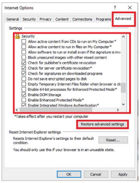
Choose Settings if you need to configure a proxy server for a connection. | Settings

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

LAN settings

OK | Cancel | Apply


Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Security

- ☐ Allow active content from CDs to run on My Computer*
- ☐ Allow active content to run in files on My Computer*
- ☐ Allow software to run or install even if the signature is inv
- ☐ Block unsecured images with other mixed content
- ☑ Check for publisher's certificate revocation
- ☑ Check for server certificate revocation*
- ☑ Check for signatures on downloaded programs
- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is cl
- ☐ Enable 64-bit processes for Enhanced Protected Mode*
- ☑ Enable DOM Storage
- ☐ Enable Enhanced Protected Mode*
- ☑ Enable Integrated Windows Authentication*

*Takes effect after you restart your computer

Restore advanced settings

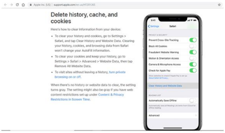
Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition. | Reset...

You should only use this if your browser is in an unusable state.

OK | Cancel | Apply

## APPLE SAFARI



Apple Inc. [US] | support.apple.com/en-us/HT201265

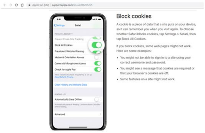
### Delete history, cache, and cookies

Here's how to clear information from your device:

- To clear your history and cookies, go to Settings > Safari, and tap Clear History and Website Data. Clearing your history, cookies, and browsing data from Safari won't change your AutoFill information.
- To clear your cookies and keep your history, go to Settings > Safari > Advanced > Website Data, then tap Remove All Website Data.
- To visit sites without leaving a history, turn private browsing on or off.

When there's no history or website data to clear, the setting turns gray. The setting might also be gray if you have web content restrictions set up under Content & Privacy Restrictions in Screen Time.

Settings
Safari
Prevent Cross-Site Tracking
Block All Cookies
Fraudulent Website Warning
Motion & Orientation Access
Camera & Microphone Access
Check for Apple Pay
Clear History and Website Data
Automatically Save Offline
Advanced



Apple Inc. [US] | support.apple.com/en-us/HT201265

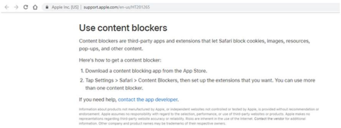
### Block cookies

A cookie is a piece of data that a site puts on your device, so it can remember you when you visit again. To choose whether Safari blocks cookies, tap Settings > Safari, then tap Block All Cookies.

If you block cookies, some web pages might not work. Here are some examples:

- You might not be able to sign in to a site using your correct username and password.
- You might see a message that cookies are required or that your browser's cookies are off.
- Some features on a site might not work.

Settings
Safari
Prevent Cross-Site Tracking
Block All Cookies
Fraudulent Website Warning
Motion & Orientation Access
Camera & Microphone Access
Check for Apple Pay
Clear History and Website Data
Automatically Save Offline
Advanced



Apple Inc. [US] | support.apple.com/en-us/HT201265

### Use content blockers

Content blockers are third-party apps and extensions that let Safari block cookies, images, resources, pop-ups, and other content.

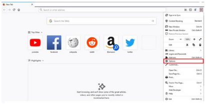
Here's how to get a content blocker:

1. Download a content blocking app from the App Store.
2. Tap Settings > Safari > Content Blockers, then set up the extensions that you want. You can use more than one content blocker.

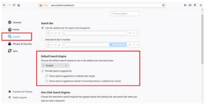
If you need help, contact the app developer.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Risks are inherent in the use of the Internet. Contact the vendor for additional information. Other company and product names may be trademarks of their respective owners.

## MOZILLA FIREFOX



Start browsing, and we'll show some of the great articles, videos, and other pages you've recently visited or bookmarked here.



about:preferences#search

Search Bar

- Use the address bar for search and navigation
- Add search bar in toolbar

Default Search Engine

Choose the default search engine to use in the address bar and search bar

Google

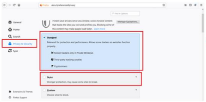
✓ Provide search suggestions

✓ Show search suggestions in address bar results

✓ Show search suggestions ahead of browsing history in address bar results

One-Click Search Engines

Choose the alternative search engines that appear below the address bar and search bar when you start to enter a keyword.



about:preferences#privacy

Protect your privacy while you browse. Block invisible content that tracks the sites you visit and profiles you. Blocking some of this content may make pages load faster. Learn more

Manage Exceptions...

Standard

Balanced for protection and performance. Allows some trackers so websites function properly.

Known trackers only in Private Windows

Third-party tracking cookies

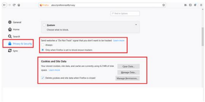
Cryptominers

Strict

Stronger protection, may cause some sites to break.

Custom

Choose what to block.



about:preferences#privacy

Custom

Choose what to block.

Send websites a "Do Not Track" signal that you don't want to be tracked. Learn more

Always [✓ Only when Firefox is set to block known trackers]

Cookies and Site Data

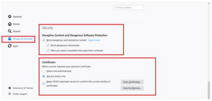
Your stored cookies, site data, and cache are currently using 6.2 MB of disk space. Learn more

✓ Delete cookies and site data when Firefox is closed

Clear Data...

Manage Data...

Manage Permissions...



Security

Deceptive Content and Dangerous Software Protection

✓ Block dangerous and deceptive content Learn more

✓ Block dangerous downloads

✓ Warn you about unwanted and uncommon software

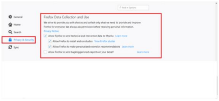
Certificates

When a server requests your personal certificate

○ Select one automatically

● Ask you every time

✓ Query OCSP responder servers to confirm the current validity of certificates



Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.

Privacy Notice

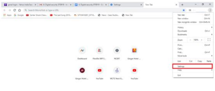
✓ Allow Firefox to send technical and interaction data to Mozilla Learn more

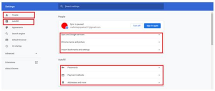
✓ Allow Firefox to install and run studies View Firefox studies

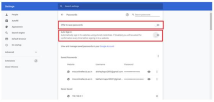
✓ Allow Firefox to make personalized extension recommendations Learn more

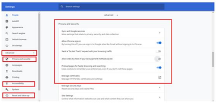
☐ Allow Firefox to send backlogged crash reports on your behalf Learn more

## GOOGLE CHROME









## Securing browsers

| | |
|---|---|
| **Google Chrome** | Click on the three vertical dot top right side corner in the Chrome and select Settings. Or simply type ***chrome://settings/*** in the address bar.<br><br>**People section**<br><br>Click on Sync and Google services<br>Check if the Safe Browsing option, which offers protection from dangerous sites, is enabled.<br><br>**Autofill section**<br><br>Click on Passwords and disable Offer to save passwords.<br>Click Payment methods and disable Save and fill payment methods.<br>Click on Addresses and more and disable Save and fill addresses<br><br>**Advanced Section**<br><br>In Privacy and security turn off the Allow sites to check if you have payment methods saved.<br>Click on Site Settings then Cookies and it is recommended to disable Allow sites to save and read cookie data (recommended) and enable Block third-party cookies. Click on Location and make sure that Ask before accessing (recommended)  is set or you can block the location access by simply toggling the button. |

## Google Chrome

Click on **Camera** and make sure that **Ask before accessing (recommended)** is set or you can block the camera access by simply toggling the button.

Click on **Microphone** and make sure that **Ask before accessing (recommended)** is set or you can block the microphone access by simply toggling the button.

Click on **Motion sensors** and **Block sites from using motion sensors by simply toggling the button.**

It is highly recommended to disable JavaScript for Security purposes but on disabling JavaScript some webpages may not load properly. To disable **JavaScript** click on JavaScript and then block it.

It also recommended to turn off Flash in Chrome. To check it click on **Flash** and make sure it showing **Block sites from running Flash (recommended).**

Click on **Pop-ups and redirects** and make sure it is Blocked, if not block it.

Click on **Ads** check it is showing **Blocked on sites that show intrusive or misleading ads (recommended).**

Click on **Clipboard** and make sure **Ask when a site wants to see text and images copied to the clipboard (recommended)** is checked.

## Apple Safari

Make sure your Safari is up-to-date to the latest version. To check for updates just go to the Apple menu and click on **Software Update.**

Now it's time to secure Safari Preferences. Just go to the **Safari Menu** and click on **Preferences.**

In General section uncheck **Open "safe" files after downloading**

Select Remove history items as **After one day.**

In the **AutoFill** section uncheck the **AutoFill web forms** options.

On the **Passwords** section and remove any stored passwords.

In the **Security** section Check **Fraudulent sites** option.

In the Web content check **Block pop-up windows.**

It is recommended to disable JavaScript for security, but some sites may not load properly.

In the bInternet plug-ins uncheck **Allow Java** and also uncheck **Allow all other plug-ins.**

In the **Privacy section**-- Select Block cookies as **From third parties and advertisers.**

Select Limit website access to location as **Deny without prompting**

## Internet Explorer

First of all, click on the Tools icon in the top right corner in Internet Explorer and click **Internet options.**
**First of all it is recommended to Update Your Windows to necessary security patches.**

In **General** section:
→ It is recommended to change the Home page first. Change it to something reputed search engine.
→ Check the Delete browsing history on exit.

In **Medium-high** section:
→ Set the Security level to High or at least Medium-high.
→ Check the box Enable Protected Mode.
→ Click on Apply

In **Privacy** Section:
→ Set the Settings to High or at least Medium High.
→ Check the boxNever allow websites to request your physical location.
→ Check Turn on Pop-up Blocker.
→ Check the box forDisable toolbars and extensions when InPrivate Browsing starts.
→ Click onApply.

**Internet Explorer**

In **Connection** Section:
→ Click on settings under theAutoComplete.
→ Uncheck Box for Forms and also for User names and passwords on forms
→ Check Ask me before saving passwords.

In **Advanced** Section:
Go for the **Security** section and select **Check for publisher's certificate revocation.**
Select **Check for server certificate revocation.**
Select **Check for signatures on downloaded programs**
Enable **Integrated Windows Authentication**
Enable native **XMLHTTP support**
Check the box of **Use SSL 2.0**
Check the box **Use SSL 3.0**
Check the box for **Use SSL 1.0**
Click on **Apply**
Click on **Ok**
Finally **restart** the Browser

**Mozilla Firefox**

To harden firefox security go fore the **three vertical lines** located in the top right corner in Firefox browser and select Options.
OR, Just type **about: preferences** in the browser address bar also.

First thing Keep your Firefox Up to date for best performance, stability and security and also make sure **Automatically install updates (recommended)** is selected in the **General section.**

In the Search section make sure you have selected a trusted search engine in the **Default Search Engine.**

In the **Content Blocking** area of **Privacy & Security** section make sure the **Standard** protection or **Strict** protection is selected. Strict protection may cause some sites to break but Standard protection will be good enough.

In **Cookies and Site Data** check the option **Delete cookies and site data when Firefox is closed.** It will delete all of your cookies after you close the Firefox browser.

Check the **Ask to save logins and passwords** for websites option in the Login and Passwords area.

Check **Use a master password.** It will pop up a window where you can set a master password. A master Password is used to protect sensitive information like site password. If you create a Master Password you will be asked to enter it once per session when Firefox retrieves saved information protected by the password.

In **History** select **Use custom settings for history** and uncheck **Remember browsing and download history** and **Remember search and form history** and also check **Clear history when Firefox closes.**

In **Permissions** Click the **Settings** right beside **Location** and add the trusted sites which can access the Location.

Click the **Settings** right beside **Camera** and add the trusted sites which can access the **Camera.**

Click the **Settings** right beside **Microphone** and add the trusted sites which can access the **Microphone.**

Check **Block websites from automatically playing sound** and also you can set exception for the sites which trust.

Check **Block pop-up windows** and also you can set exception for the sites which trust.

Check **Warn you when websites try to install add-ons** to prevent anty third party website to install add-ons in the browser.

In the **Firefox Data Collection and Use** uncheck **Allow Firefox to send technical and interaction data to Mozilla**

Uncheck **Allow Firefox to make personalized extension recommendations.**

Uncheck **Allow Firefox to send backlogged crash reports on your behalf.**

| | |
|---|---|
| **Mozilla Firefox** | In the **Security** make sure that **Block dangerous and deceptive content** is checked.<br><br>Check **Block dangerous downloads** option.<br><br>Check **Warn you about unwanted and uncommon software.**<br><br>Select **Ask you every time** when a server requests your personal certificate.<br><br>Check **Query OCSP responder servers to confirm the current validity of certificates.**<br><br>Always install Plugins and Extensions from official Mozilla foundation. To install add-ons in Firefox go to Add-ons by going that three vertical lines mentioned earlier and install as per your requirements |

### *8.3.4 Beware of strangers and suspicious links*

Pause and think carefully before clicking on the links in email, messages or on social networking sites. Do not click on the links in messages if the sender is unknown or if the message is unexpected.

If a link looks suspicious or you cannot tell where it leads to, before you click hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognize or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video, or webpage without clicking the suspicious link.

Expand shortened URLS to check if they are safe. Short URLs are often used in social media. There are a number of services that create short links - such as goo.gl, bit.ly, tinyurl.com, ow.ly and youtu.be. To check if these links are safe you can use an 'expand link' facility to get the original URL from a shortened link without having to click through to the destination. Look for a short URL expander that is recommended by your anti-virus software or a reputable software company.

Be wary of offers that seem too good to be true. Leave websites that ask for your personal or banking details in return for money – these are scams. Remember, if it seems too good to be true, it probably is not.

Only download files and applications from websites that you trust, such as from official app stores or legitimate organisations, such as your bank.

a) While downloading any file close all the applications that are running on your computer, let only one set-up file run at a time of downloading.

b) Set firewalls, set antivirus to actively scan all the files you download.

c) Scan all the files after you download whether from websites or links received from emails.

d) Always use updated antivirus, spam filters and spyware to detect and remove viruses and spywares from the application you want to download.

e) Never download any files like music, video, games and many more from untrusted sites and don't go by the recommendations given by your friends or made by any random website's comments.

f) Check that the URLs are the same and always download games, music or videos from the secure websites like which use HTTPS websites instead of HTTP. In the web address, it replaces "http" to "https". The https refers to the hypertext transfer protocol secure.

g) Download anything only from trustworthy websites. Do not click on the links to download anything from unauthorized sites.

h) If any dirty words appear on the website just close the window no matter how important it is, because spyware may be installed on your PC from such websites.

i) Check the size of the file before you download, sometimes it shows a very small size but after you click it increases the size of the file.

j) Don't accept anything that offers you free download because that may contain malicious software.

k) Don't click the link or file and let it start downloading automatically, download the file and save where you want to save and then run on the application.

l) Set secure browser settings before you download anything.

m) Read the terms and conditions carefully before you click on install or run applications.

n)Do not download anything until you know complete information of the website and know whether it is an original site of an original company.

o) Never download from the links that offer free antivirus or anti spyware software, always download from trusted sites, if you are not sure about the site you are downloading, enter the site into favourite search engine to see anyone posted or reported that it contains unwanted technologies.

### *8.3.5 Regular data back-ups*

Taking regular data backups is an important strategy for securing all your important data. A backup is the only way to restore the original data.

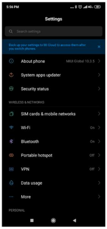
**Why you must have Data Backup**

Data on a hard disk can be lost for a variety of reasons, such as:-

- hardware failure;
- operating system failure, e.g., file system crash;
- files or volumes modified or deleted accidentally by yourself;
- files or volumes modified or deleted intentionally by intruder;
- files or volumes modified or deleted by virus or malicious codes.

## Back ups

You can also take a backup of your data to keep it safe.
Many companies like Apple, Xiaomi, Samsung have inbuilt backup features in their phones.
You can find the option in the settings, as shown below.


5:56 PM

Settings

Search settings

Back up your settings to Mi Cloud to access them after you switch phones.

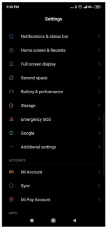
About phone — MIUI Global 10.3.5
System apps updater
Security status

WIRELESS & NETWORKS

SIM cards & mobile networks
Wi-Fi — On
Bluetooth — On
Portable hotspot — Off
VPN — Off
Data usage
More

PERSONAL

*Step 1: Go to Settings*


5:56 PM

Settings

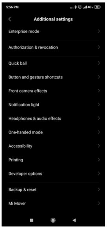
Notifications & status bar
Home screen & Recents
Full screen display
Second space
Battery & performance
Storage
Emergency SOS
Google
Additional settings

ACCOUNTS

Mi Account
Sync
Mi Pay Account

APPS

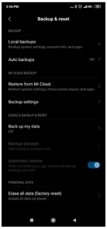
*Step 2: Go to additional settings*


5:56 PM

Additional settings

Enterprise mode
Authorization & revocation
Quick ball
Button and gesture shortcuts
Front camera effects
Notification light
Headphones & audio effects
One-handed mode
Accessibility
Printing
Developer options
Backup & reset
Mi Mover

*Step 3:*
*Go to Backup and Reset*


5:56 PM

Backup & reset

BACKUP

Local backups
Backup system settings, account info, and apps
Auto backups — Off

MI CLOUD BACKUP

Restore from Mi Cloud
Restore system settings, Home screen layout, and apps
Backup settings

GOOGLE BACKUP & RESET

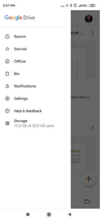
Back up my data
Off
Backup account
Add a backup account now
Automatic restore
When reinstalling an app, restore backed-up settings and data

PERSONAL DATA

Erase all data (factory reset)
Erases all data on phone

*Step 4:*
*Choose the relevant options*

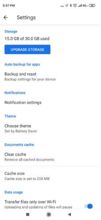
## You can also use Google Drive to take a backup of your data.


5:57 PM

Google Drive

Recent
Starred
Offline
Bin
Notifications
Settings
Help & feedback
Storage
15.0 GB of 30.0 GB used

Step 1: Open Google Drive. Click on the three lines on the left top corner to open Settings


5:57 PM

Settings

Storage
15.0 GB of 30.0 GB used
UPGRADE STORAGE

Auto-backup for apps
Backup and reset
Backup settings for your device

Notifications
Notification settings

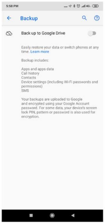
Theme
Choose theme
Set by Battery Saver

Documents cache
Clear cache
Remove all cached documents

Cache size
Cache size is set to 250 MB

Data usage
Transfer files only over Wi-Fi
Uploading and updating of files will pause

Step 2: Click on Backup and Reset


5:58 PM

Backup

Back up to Google Drive

Easily restore your data or switch phones at any time. Learn more

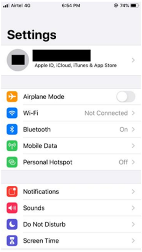
Backup includes:

Apps and apps data
Call history
Contacts
Device settings (including Wi-Fi passwords and permissions)
SMS

Your backups are uploaded to Google and encrypted using your Google Account password. For some data, your device's screen lock PIN, pattern or password is also used for encryption.

Step 3: Turn on the option. Your data will now be stored on Google drive as well.

## Backup on iPhones:


Airtel 4G 6:54 PM 74%

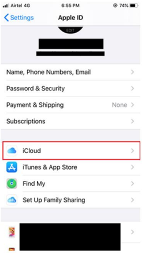
Settings

[redacted]
Apple ID, iCloud, iTunes & App Store

Airplane Mode
Wi-Fi Not Connected
Bluetooth On
Mobile Data
Personal Hotspot Off

Notifications
Sounds
Do Not Disturb
Screen Time

Step 1: Go to Settings


Airtel 4G 6:55 PM 74%

Settings Apple ID

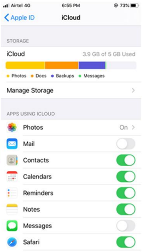
EDIT
[redacted]

Name, Phone Numbers, Email
Password & Security
Payment & Shipping None
Subscriptions

iCloud
iTunes & App Store
Find My
Set Up Family Sharing

[redacted]

Step 2: Click on iCloud.


Airtel 4G 6:55 PM 73%

Apple ID iCloud

STORAGE
iCloud 3.9 GB of 5 GB Used
● Photos ● Docs ● Backups ● Messages

Manage Storage

APPS USING ICLOUD
Photos On
Mail
Contacts
Calendars
Reminders
Notes
Messages
Safari

Step 3: Take backup of all the applications that you wish to.

### *8.4 Personal security*

#### *8.4.1 Protect personal information*

Do not share your personal information like date of birth, address, and phone number on social media or other online platforms.
Create usernames that never reveal true identity

#### *8.4.2 Beware of strangers*

A cyber groomer may create a fake account to befriend victims.

Avoid talking to people who ask you questions related to your physical or sexual experiences. You can tell the person to stop asking you such questions as you feel uncomfortable. If they continue to do the same, immediately inform your parents or elder. Do not feel that your parents will restrict your online activity or ask you not to use your computer or smartphone. It is important to inform them so that they can support and guide you to prevent potential harm.

Ignore friend requests from unknown people on social media platforms.
Be cautious when your chat partner gives you many compliments regarding your appearance within a short span of your acquaintance.

Do not talk to people who ask you to share your sexually explicit photographs or videos. If you share your sexually explicit photos or videos with someone, the person can share those photos with others or post them on social media. They can also blackmail you.

Never turn on your webcam if your chat partner does not connect to the webcam. Keep your webcam private. Put a sticker over your webcam, laptop camera, or phone camera when they aren't in use. These devices can sometimes be hacked and used to take pictures or videos of you without your consent.

Never install unwanted Software and Apps like dating App, online games, etc. from unknown sources.

Do not agree to friend requests from unknown people on social media networks –

People are not always who they say they are. Learn more about protecting yourself when using social media.

You should be very careful in the chat rooms. Never share personal details and limit your identity.

a) **Protect your online reputation:** Use the services provided to manage your digital footprints and 'think before you post'. Even if offensive posts and pictures are removed by appealing to the service providers, the possibility of someone taking screenshots or downloading the content cannot be ruled out.

b) Do not go to meet a person whom you met online alone. Always take a friend or an elder person with you.

#### *8.4.3 Learn to block*

Do not accept friend requests from unknown people on social media platforms. As a rule-of-thumb, only add people online who you know offline
A cyber bully can even create a fake account to befriend victims.

#### *8.4.4 Abide by the law*

Use reliable services and know how to legally access the music, film and TV you want.

**Acknowledge your sources:** use trustworthy content and remember to give credit when using others' work/ideas

### *8.4.5 Take any feeling of discomfort seriously*

Have you been in the following situations:
Online conversations with a person, known or unknown, are making you feel uncomfortable?
Someone is stalking you online.
Do not give in to pressure: If you lose your inhibitions, nerve and temper, you have lost control. Exercise control by using the blocking and reporting features provided by various platforms. Express your discomfort and, if need be, discontinue the conversation. If it does not help, block that person. If the pestering and harassment becomes threatening, report.

Seek advice from a trusted adult.

### *8.4.6 Seek help*

Know where to find help: Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it is never too late to tell someone.

Talk to your elders or parents, if your chat partner suggests to keep your conversation with them a secret.

You can also report these to Childline at 1098.

You can protect yourself from becoming a victim of grooming:

a) Take all precautions about sharing personal information and identity details during chats or in public spaces.

b) If groomer is using social media platforms to groom you, you can block him/her. All the social media apps or services have the option to block a user.

c) Save messages, pictures or videos shared with you by the groomer. Such messages, pictures or videos can be used as an evidence to initiate legal action.

d) Your parents/elders can contact local police station to lodge a complaint against the groomer.

Do check with your parents before downloading apps or sharing personal information

This is mandatory for anyone below the age of 14. Some apps are malicious in nature. Therefore, to prevent malpractices, it is important to share the information with parents.

Also, Facebook policy does not allow any student below the age of 14 to use the app. Even Netflix, YouTube and Amazon Prime mandates 'Kids mode' for all children below the age of 14.

***Dealing with unauthorized access***

**Giving Permissions to apps:** While installing apps, give only those permissions that are absolutely essential for the functioning of the apps. Of any application does not function without all permissions, it is best to not install it.

**Sharing the device's location:** Always allow those app with device location permission which actually required.

**Via GPS:**

**Via Geotagging:** Link your location with your posts, only when you are sharing it with people that you know and trust. sharing your location with strangers or merely making it public may compromise your security.

Certain characteristics of the digital environment magnify the risk that children will be exploited or abused by other users. In particular, online abusers can easily operate anonymously and bypass gatekeepers such as parents or teachers. When children are bullied online, such as through 'revenge porn', their humiliation can be very public.

**Online grooming:** deceiving a child for sexual purposes – is on the rise, although its extent remains unknown. The sexual abuse that follows may be online, such as by 'sexting' – sending or eliciting explicit sexual images – or offline, if the victim is lured into a meeting.

**Cyber-bullying,** which takes several forms is becoming more common and can have a profound impact on mental health, well-being, and educational attainment. When children go online they are more likely to bully others, and to be bullied, than when they are offline.

**Consent.** Empower children to decide for themselves how others collect and use their information by requiring their consent. As of now, there is no minimum age of digital consent in India.

WATCH

***https://www.youtube.com/watch?v=q6xzoWCJJ44***

# 9. Digital Law

### *9.1 What is digital law?*

Digital law can be defined as the legal rights and restrictions governing technology use.

They are criminals, breaking the law, either knowing or not knowing, what is appropriate or inappropriate technology use.

Most users neither know nor understand the impact or the possible consequences of some of their online activities. Everyone needs to be aware that certain rules apply to anyone who uses any online devices for any purpose, and there are legal implications of some of their online actions. If you are caught and proved guilty, you attract penalties such as hefty fine or imprisonment.

The following are some actions that are unethical and illegal.

• Software or systems piracy,
• Downloading music and films without authorisation or payment,
• Stealing other people's work (plagiarism and copyright infringement), personal data (identity theft), and property online
• Illegal file sharing,
• Hacking into others' systems or networks,
• Creating destructive viruses, worms or trojan horses, and causing damage to other people's devices and data,
• Sending spam,

***Golden rules***

• *Think before you act. You may be violating the law of the land.*
• *Ignorance of the law is not a valid defence in legal fora.*
• *What is ethical is generally legal.*

### *9.2 Illegal activities using digital technologies*

Plagiarism is an act or instance of using or closely imitating the language and thoughts of another author without authorization, and the representation of that author's work as one's own, as by not crediting the original author. It is tantamount to stealing other people's work, using words, ideas, images or data of another person without attributing the source is both unethical as well as illegal. It constitutes a violation of intellectual property rights. Be honest about the online (and even offline) resources you use as part of completing any school assignment, project, essay or presentation. Acknowledge or give credit if you do so.

Students have so much data and resources available at their fingertips which makes school project work much easier than ever before. The ease and speed with which anyone can share, download and use digital information has also made it very easy to violate the law intentionally or unintentionally. When a person uses someone else's creative work and passes it off as his or her own, it is regarded as a copyright infringement. If you publish a story online, and you use a photograph you found on the Internet, but you do not get the photographer's permission to use that photo, or have not paid for it you have infringed on that photographer's copyright.

There is, however, a difference between plagiarism and copyright violation. Plagiarism involves copying someone else's work without acknowledging or giving them credit whereas copyright infringement involves using someone else's work but not paying them for it. While plagiarism is an ethical problem that can affect academic and professional reputations, copyright infringement is a violation of law, which can attract penalties.

***Fair use*** is an exception to the restrictions imposed by copyright law. Quoting a few lines from a copyrighted work in an academic paper with proper citation generally qualifies as "fair use". Do remember:

• The purpose of the work should be academic, not-for-profit, and educational.
• The piece is not copied in its entirety. A few lines from the original are quoted.
• The reference does not have any impact on the value of the original work.

### 9.2.2 *Sexting*

Messaging of sexually explicit content by way of images, photos, clips, video files or other material can increase the vulnerability of children and young people manifold. Many children participate willingly in conversations with subtle or explicit sexual undertones, and may not object to such messages either of their own volition or due to peer pressure.

The growing number of such reported cases of sexting and self-exposure highlight the vulnerability of children and young people to blackmail and extortion (including "sextortion") and "revenge porn". Even if this is being done by mutual consent among children, some of these activities are punishable by law and can lead you into further exploitation by anyone who gets hold of these messages or images. Remember, once online, information may become perpetual.

Victimizing by way of revenge porn is often practiced by children below 18 years of age. It may be described as "an act whereby a perpetrator satisfies his anger and frustration for a broken relationship through publicizing false, sexually provocative portrayal of his/her victim, by misusing information that he may have known naturally and that he may have stored on his computer, or phone, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to publicly defame the victim.[6]

### 9.2.3 *Online child abuse and exploitation*

There is global consensus that child sexual abuse and exploitation is unacceptable offline or online. Under no circumstances is the production, distribution and viewership of sexually explicit images of children is permitted. The law imposes strict penalty and punishment on anyone found to be taking, sharing and viewing such pictures.

### 9.2.4 *Defamation*

Social media, email groups, intranet, bulletin boards, chats and other digital spaces enable widespread dissemination of offensive content against a person. Online publication of defamatory statements about a person can be more harmful and damaging than verbal and offline statements. The effects of online communication of sensitive personal information, images or videos can be devastating and intimidating for children in particular.

Offensive messages, name calling and body shaming on social media can be very hurtful. The severity, frequency and the fact that such messages spread so fast cause a lot of distress to the person who has been targeted. Even though it may be difficult to establish such behaviour as an offence under Indian law, it is grossly unethical to threaten or humiliate anyone online. The persons who commits this offence may evade legal penalties but will project themselves as bully. They also remain at high risk of leaving their digital footprints and spoil their reputation.

## 9.3 *Legal penalties for online offences*

Indian laws deal with many of the core issues related to digital technologies. You need to understand that some of your online actions may be on the borderline of an offence and some may actually be infringing the law.

| **Illegal online activity** | **Laws covering offense** | **Penalty** |
|---|---|---|
| *Posting or sharing of inappropriate images and comments online or through WhatsApp.* | *Protection of Children Against Sexual Offences Indian Penal Code, Information Technology Act, 2000* | *A term of up to 3-5 years imprisonment and also a fine* |
| *Revenge porn*<br>*If an inappropriate picture or explicit selfie has been shared by a friend, for taking revenge threatening to circulate this to a wider group or demanding a favour for not doing so* | *POCSO, 2012*<br>*Indian Penal Code* | *A term of up to 7 years imprisonment with a fine*<br><br>*In case of extreme effect of the said act like committing suicide or attempt to commit suicide, the punishment may go upto life term as well* |

[6] *Halder and Jaishankar, 2013*

| **Illegal online activity** | **Laws covering offense** | **Penalty** |
|---|---|---|
| *Violation of privacy*<br>*Uses any electronic device and/or online medium to record, circulate, transmit, publish or bring into the public domain any image, photograph, film, videotape, MMS etc. that has private parts of a child captured in violation of his privacy commits the offence of 'Violation of privacy of a child'.* | *IT Act 2000*<br>*POCSO Act, 2012* | *A Term of upto 7 years imprison-ment or a fine or both* |
| *Impersonation*<br>*Sending someone messages by assuming a false identity.* | *Information Technology Act, 2000* | *A term of up to 3 years imprison-ment and also a fine* |
| *Unauthorised access*<br>*Hacking someone's computer, email or social networking account* | *Information Technology Act, 2000* | *A term of up to 2-3 years imprison-ment or fine or both* |
| *Online piracy*<br>*Downloading movies and music for free.*<br><br>*Illegally copying or distributing software using the internet without the consent of the rights owner.* | *Copyright Act, 1957* | *Punishment of a term up to 6 months to 3 years of imprisonment and fine* |
| *Plagiarism*<br>*Using words, ideas, images or data of another person without attributing the source.* | *Copyright Act, 1957* | *A term of imprisonment from 6 months to 3 years and fine* |
| *Misrepresentation*<br>*Falsification of age for the purpose of creating accounts or accessing certain websites. It amounts to entering under a contract with the service provider based on misrep-resentation of facts and real identity.* | *Indian Penal Code* | |
| *Defamation*<br>*Posting defamatory statements, images or videos, about a person on social media, chats, bulletin boards or any digital space* | *Indian Penal Code* | *A term of upto 2-3 years imprison-ment , or fine, or both* |

Although there are legal provisions to address online offences, there are loopholes in the laws. It needs to be recognised that legislation is often unable to keep up the pace of technological developments. A new set of problems emerges before appropriate legal provisions can be enacted. Furthermore, there are difficulties in implementing national laws, especially when the internet does not recognise national boundaries. Indian laws apply to the territory of Indian state, whereas the servers of internet service providers are located in the US and western Europe. Although legal remedies must be pursued in serious cases, prevention through safe online behaviours is currently the best option available.

### 9.4 *Good practices*

What you should right is clearly your prerogative. But do remember that any production, consumption and distribution of content which involves sexual imagery of children is illegal.

**Being safe on social media platforms**

***Facebook***

***Choose friends wisely.*** *Everything is not about the number of friends you have. Select your friends wisely as they can access your information. Learn to delete/block unwanted friends.*

***Think before saying anything.*** *Be mindful of what you post/update on Facebook. Ask if you will regret it five years later. Do not become a part of hate-groups.*
*Manage privacy settings. Your posts are publicly shared unless you go to settings and change your Security and Privacy to Only Friends.*

***Keep in mind the dangers of sharing.*** *Be careful of what information you put out on Facebook. Check your posts and images for indicators of your whereabouts or anything that may invite unwanted users.*

***Create friends lists to manage your posts.*** *Create separate lists for your acquaintances, friends, family etc. This will make it easy to regulate or control who can see your posts.*

***Look out for suspicious activities.*** *Do not click on suspicious links. Beware of fake Facebook pages that steal your password. If your account is hacked, change your password or report to Facebook*

***Instagram***

***Consider the whole image.*** *Ask yourself if the image or the background giving an indication where you were or what you were doing at the time of taking the picture. If yes, then reconsider posting it.*

***Manage your visibility.*** *Photos you are tagged in are visible to everyone. To make it secure you can make your account private by going to the menu on the (top right side) on your profile.*

***Accepting followers.*** *If your account is private you can approve who follows you. Do not accept requests from strangers. Also be mindful of who you are following.*

***Block/report unwanted contacts.*** *Go to their profile and tap menu (top right side) to report and block. You can also report images by going to menu option at the top of each image.*

***"Untag" yourself.*** *You can untag yourself by tapping on your username in the post, provided the post is public or you follow the person who tagged you.*

***Other tips.*** *Switch off geotagging and location feature. Delete your post if you are not sure about it. Posts are easy to embed in other websites. It may go viral.*

***Snapchat***

***Screen capture is possible*** *even on Snapchat, which does not save images. Screen shots are an easy way to save images, and many third party apps auto-save images.*

***Notification is not guaranteed.*** *Snapchat tells you when your snap was viewed or screenshot. But this function is not always reliable.*

***Manage your privacy settings.*** *Tap on the ghost icon on the top of your camera screen-> Settings (gear icon)-> 'who can' section-> change settings from Everyone to My Friends*

***Threat of unknown users.*** *Tap and hold the user and select gear icon to Block unwanted users.' Add Nearby' may seem cool but keep in mind it can be risky.*

***Sexting concern.*** *Avoid sharing snap stories that you do not want others to access. Do not share sexually explicit pictures as these may easily go viral.*

***Keep your User ID Private.*** *Do not post your username on social media as it may attract unwanted attention. Also do not share your password with anyone.*

***Source: www.aarambhindia.org; https://infosecawareness.in/home/index.php***

***Other instant messaging applications***

*Do not open, accept, or download a file in Instant Messenger from someone you do not know or if you do not know what is in the file.*

*Contact the sender by email, phone, or some other method to confirm that what they sent was not a virus.*

*Visit Microsoft Update to scan your windows computer and install any high-priority updates that are offered to your PC. If you have Automatic Updates enabled, you have to make sure you install them when received.*

*Use up-to-date version of your Instant Messenger software for better protection of your computer against viruses and spyware.*

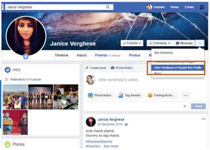
*Upgrade from MSN Messenger to Windows Live Messenger in order to block attachments that may contain malware and allow scanning of attachments for viruses.*

*"Spim" (a short form of spam over instant messaging) uses IM platforms to send spam messages over IM. Like email spam messages, a spim message may contain advertisements or weblinks, by clicking on those links malicious code enters into your PC.*

*Anti-spyware software can protects the digital device and helps in removing any spyware you may already have. Windows Defender may be downloaded in the absence of anti-spyware software.*

### *9.5 Available redressal mechanisms*

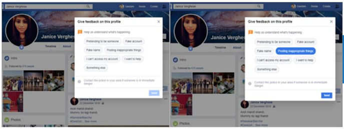
#### *9.5.1 Social media platforms*



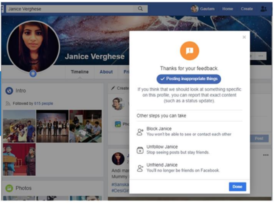
Janice Verghese
22 December 2018

Andi mandi shandi,
Mummy ko lagi thandi.
#SanskariBacche
#DesiGirl... See more

*Step 1: If you wish to report any account/post/comment, go to the 3 dots on the right top corner of the account/post/comment. When you click on the dots, you will find the option "Give Feedback or Report". Click on it.*


Give feedback on this profile
Help us understand what's happening
Pretending to be someone
Fake account
Fake name
Posting inappropriate things
I can't access my account
I want to help
Something else
Contact the police in your area if someone is in immediate danger.
Send

*Step 2: You will be presented with a list of reasons to ascertain why you wish to report that content.*



Thanks for your feedback.

If you think that we should look at something specific on this profile, you can report that exact content (such as a status update).

Block Janice
You won't be able to see or contact each other

Unfollow Janice
Stop seeing posts but stay friends.

Unfriend Janice
You'll no longer be friends on Facebook.

*Step 3: Choose the appropriate reason and click on "Done".*

*Facebook will remove the account/post/comment if it violates the community guidelines of the platform.*

***INSTAGRAM***

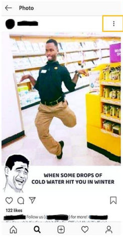
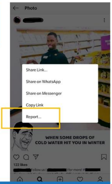


Photo
WHEN SOME DROPS OF COLD WATER HIT YOU IN WINTER
122 likes
Follow us ([redacted]) for more! [redacted]

*Step 1: If you come across any content that you wish to report, or get removed, go to the top right corner of the post and you will find three dots.*



*Step 2: When you click on the dots, you will find the option to "Report"*

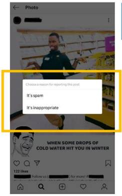
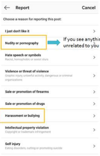


Photo
Choose a reason for reporting this post:
It's spam
It's inappropriate
WHEN SOME DROPS OF COLD WATER HIT YOU IN WINTER
122 likes

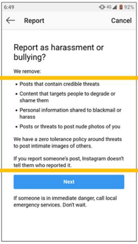
*Step 3: Choose "Spam" of you are reporting commercial content (like advertisments). if what you are reporting is not an ad, choose "It's inappropriate".*

*Step 4: Once you click on "Report", you will be presented with a list of reasons to ascertain why you wish to report that content.*


Report
Cancel
Choose a reason for reporting this post:
I just don't like it
Nudity or pornography
Hate speech or symbols
Racist, homophobic or sexist slurs
Violence or threat of violence
Graphic injury, unlawful activity, dangerous or criminal organizations
Sale or promotion of firearms
Sale or promotion of drugs
Harassment or bullying
Intellectual property violation
Copyright or trademark infringement
Self injury
Eating disorders, cutting or promoting suicide

If you see anything obscene unrelated to you

If anybody is bullying YOU or blackmailing YOU



6:49

Report Cancel

Report as harassment or bullying?

We remove:

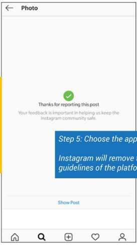
- Posts that contain credible threats
- Content that targets people to degrade or shame them
- Personal information shared to blackmail or harass
- Posts or threats to post nude photos of you

We have a zero tolerance policy around threats to post intimate images of others.

If you report someone's post, Instagram doesn't tell them who reported it.

Next

If someone is in immediate danger, call local emergency services. Don't wait.



Photo

Thanks for reporting this post

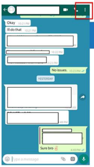
Your feedback is important in helping us keep the Instagram community safe.

Show Post

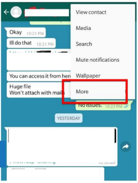
*Step 5: Choose the appropriate reason and click on "Next".*

*Instagram will remove the content if it violates the community guidelines of the platform.*

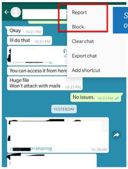
***WHATSAPP***



*Step 1: If you wish to report any number on WhatsApp, go to the 3 dots on the right-top corner of the chat.*



*Step 2: When you click on the dots, you will find the option "More". Click on it.*


[redacted]

Report

Block

Clear chat

Export chat

Add shortcut

Okay 10:21 PM

Ill do that 10:21 PM

[redacted]

You can access it from here

Huge file
Won't attach with mails 10:23 PM

No issues. 10:23 PM

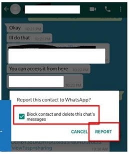
YESTERDAY

[redacted]

/[redacted]p=sharing 10:38 AM

[redacted]

Step 3: You will then see the option to "Report". Click on it.


[redacted]

Okay 10:21 PM

Ill do that 10:21 PM

[redacted]

You can access it from here 10:22 PM

[redacted] 10:23 PM

Report this contact to WhatsApp?

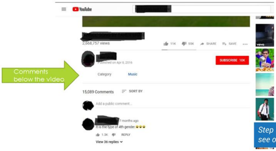
[✓] Block contact and delete this chat's messages

CANCEL REPORT

/view?usp=sharing 10:38 AM

Step 4: You can block the person as well when you report their account. Once reported the account may be deleted if it violates the community guidelines of the platform.

## YOUTUBE



[redacted]

[redacted]

2,668,757 views

11K 55K SHARE SAVE

[redacted]

Published on Apr 8, 2016

SUBSCRIBE 10K

Category Music

15,089 Comments SORT BY

Add a public comment...

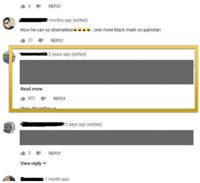
[redacted] 7 months ago

It is the type of 4th gender 😀😀😀

1.3K REPLY

View 36 replies

Step 1: If you wish to report any comment you see on YouTube, go to the comment section.


9 REPLY

[redacted] months ago (edited)

How he can so shameless😀😀😀😀 , one more black mark on pakistan

21 REPLY

[redacted] 2 years ago (edited)

[redacted]

Read more

851 REPLY

View 40 replies

[redacted] 2 days ago (edited)

[redacted]

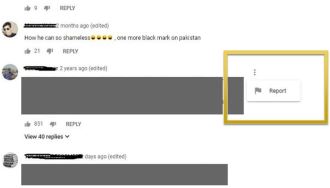
3 REPLY

View reply

[redacted] 1 month ago

Step 2: Next to the comment you wish to report, you will find 3 dots on the right top corner.

*Step 3: When you click on the dots, you will find the option to "Report"*



9 REPLY

[redacted] 2 months ago (edited)

How he can so shameless😀😀😀😀 , one more black mark on pakistan

21 REPLY

[redacted] 2 years ago (edited)

[redacted]

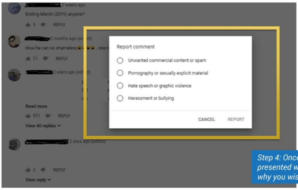
851 REPLY

View 40 replies

Report

[redacted] days ago (edited)

[redacted]



[redacted] 2 weeks ago

Ending March (2019) anyone?

9 REPLY

[redacted] 2 months ago (ed d)

How he can so shameless😀 😀😀 , one

21 REPLY

[redacted] 2 years ago (ed d)

Read more

851 REPLY

View 40 replies

[redacted] 2 days ago (edited)

2 REPLY

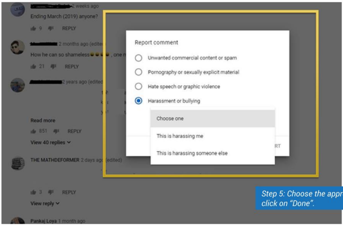
View reply

Report comment

- Unwanted commercial content or spam
- Pornography or sexually explicit material
- Hate speech or graphic violence
- Harassment or bullying

CANCEL REPORT

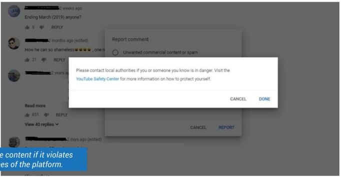
*Step 4: Once you click on "Report", you will be presented with a list of reasons to ascertain why you wish to report that content.*


[redacted] 2 weeks ago
Ending March (2019) anyone?
9 REPLY
[redacted] 2 months ago (edited)
How he can so shameless , one
21 REPLY
[redacted] 2 years ago (edited)
Read more
851 REPLY
View 40 replies
THE MATHDEFORMER 2 days ago (edited)
3 REPLY
View reply
Pankaj Loya 1 month ago

Report comment
- ○ Unwanted commercial content or spam
- ○ Pornography or sexually explicit material
- ○ Hate speech or graphic violence
- [✓ Harassment or bullying]

Choose one
This is harassing me
This is harassing someone else

*Step 5: Choose the appropriate reason and click on "Done".*


[redacted] 2 weeks ago
Ending March (2019) anyone?
9 REPLY
[redacted] 2 months ago (edited)
How he can so shameless , one
21 REPLY
[redacted] 2 years ago
Read more
851 REPLY
View 40 replies
[redacted] 2 days ago (edited)

Report comment
○ Unwanted commercial content or spam
CANCEL REPORT

Please contact local authorities if you or someone you know is in danger. Visit the YouTube Safety Center for more information on how to protect yourself.

CANCEL DONE

*YouTube will remove the content if it violates the community guidelines of the platform.*

**Social media platforms have similar processes** for reporting objectionable photos, videos, accounts and comments or any other content. Click on the three dots on the corner of the post to go to the "report" option. Report objectionable content by choosing the appropriate reason.

*Twitter:*
*https://help.twitter.com/en/contact-us*

*For Facebook:*
*https://m.facebook.com/help/*

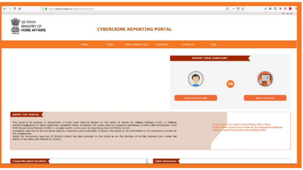
*Instagram:*
*https://help.instagram.com/*

*Youtube:*
*https://www.youtube.com/t/contact_us*

### 9.5.2 *Police*

**Reporting on cybercrime.gov.in**

Portal run and maintained by Ministry of Home Affairs, Government of India



गृह मंत्रालय MINISTRY OF HOME AFFAIRS

CYBERCRIME REPORTING PORTAL

Home FAQs Online Safety Tips Feedback Contact Us Help

REPORT YOUR COMPLAINT

Report Anonymously OR Report and Track

ABOUT THE PORTAL

This portal is an initiative of Government of India under National Mission for the safety of women by utilising Nirbhaya funds, to facilitate victims/complainants to report cybercrime complaints online. At present this portal caters to complaints pertaining to online Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content.
Complaints reported on this portal are dealt by respective police authorities of States/ UTs based on the information in the complaints provided by the complainants.
Option for anonymous reporting of CP/RGR content has been provided on this portal as per the direction of Hon'ble Supreme Court under the matter of Suo Moto Writ Petition no.3/2015.

If you want to report something other than Cybercrime cases or in case of an emergency please contact your local police by dialing 100.

Frequently Asked Questions

Cyber Awareness

Log into the cybercrime portal of the Ministry of Home Affairs
*https://cybercrime.gov.in/cybercitizen/home.htm*

The Ministry of Home Affairs, Government of India, has set up a portal to facilitate online complaints of cybercrimes, including online child pornography, child sexual abuse materials, and sexually explicit content (e.g., sexual harassment, abuse, rape and gang rape). Police authorities of relevant states and union territories initiate investigations and legal processes based on the information provided by the complainants. The portal also has the option for anonymous reporting of child pornography and sexually explicit content.

***Reporting to the police cyber cell***
Children, parents or other concerned adults on their behalf, can approach the cyber cells of the State police to report any online offence. Unlike other crimes, cyber-crimes are not limited by jurisdiction. You can report to the cyber-cell of any city, even if the offense was committed when you were in a different city.

***Filing an FIR with the local police***
In case you are unable to file a complaint in the cyber cell, you can file an FIR with the local police station. It is not necessary to know the name of the person responsible for the crime to lodge an FIR. Tell the police whatever you know. The local police is expected to coordinate with the cyber cell in the investigation and legal processes.

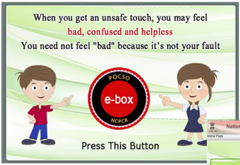
### *9.5.3 Childline 1098*

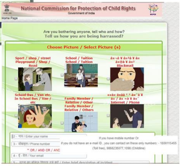
CHILDLINE 1098 is India's first 24-hour, free, emergency phone service for children in need of aid and assistance. A child or any adult on his or her behalf can dial 1098, the toll free number to seek help for emergency needs and to avail of long-term care and rehabilitation services.

### *9.5.4 NCPCR and SCPCRs*

Log into the POCSO E-box
The National Commission for the Protection of Child Rights (NCPCR) set up this online portal to receive complaints regarding sexual abuse and related offences. A child or an adult on his or her behalf can locate the POCSO e-box at the NCPCR site

*http://www.ncpcr.gov or http://www.ncpcr.gov.in/index2.php. It will navigate to a page with the window having a short animation film.*


When you get an unsafe touch, you may feel
bad, confused and helpless
You need not feel "bad" because it's not your fault


National Commission for Protection of Child Rights
Government of India

Are you bothering anyone, tell who and how?
Tell us how you are being harrassed?

Choose Picture / Select Picture (s)

2 - नाम / Enter your name
3 - मोबाइल / Phone number
* OR / AND OR / AND
4 - ई - मेल / Your email
If you have mobile number Or
If you do not have an e-mail ID , you can contact on these only numbers: - 1800115455 (Toll free), 9868235077,1098 (Childline)

***9.6 Reporting***

· Social- Talk to parents, teachers , counsellors
· Legal- Approach the police
· Platform - in app reporting, as discussed above

***Content Removal from Websites***

If ever any photo or video of yours (that you clicked or appear in), is shared online onto a website without your consent, it can be removed by following the process given below:

1. Find the relevant page or email address for initiating the DMCA request. For example: Search 'Platform/Service name' DMCA on Google. (For eg. Search for "FacebookDMCA" on Google).

2. Carefully open the links suggested on the search page and find either the email address or a form that can be filled.

3. Complete the form to send a DMCA takedown request.

4. If you find an email address, (like contact@abc.com, abuse@abc.com), send an email with Subject 'DMCA Takedown Request' and write clearly about the content and its location (URL or the link to the photo/video) on the platform that you want to remove

***Stop...Review...Post***
***Stop...Review...Report***
***Stop...Review...Block...Report***

## *Being Smart Online Checklists*

**Checklist: How to keep the devices safe?**

**I. Be alert**
*Keep the devices clean*

a) Ensure you keep your internet-connected devices, like laptops, phones and tablets, safe from malware.
b) Make sure software of operating systems is up-to-date. Also make sure security software that updates automatically is installed on devices.

**II. Keep devices safe**
*Mobile phones*

a) Use a screen lock to lock your smartphone
b)Protect sensitive data by taking regular backups either on Dropbox, OneDrive or iCloud
c) Always switch off your wireless connections e.g. Bluetooth,Wi-Fi, NFC, etc. When not in use.
d) Use genuine web browsers and never save your login credentials, banking details
e) Install an antivirus on your smartphone

**III. Be smart**
*Manage mobile apps:*

a) Keep apps on your mobile devices updated. Updates often have security fixes in them.
b) Delete apps you no longer use. It would also entail clearing of the cache

# USEFUL CONTACTS

## *I. Police Cyber cells*

| Nodal CyberCrime Portal | | | | Grievance Officer Details | | | |
|---|---|---|---|---|---|---|---|
| **Name** | **Rank** | **Landline** | **Email** | **Name** | **Rank** | **Landline** | **Email** |
| Ms. D Mary Prasanthi | SP | 0863-2340063 | cybercrimes-cid@ap.gov.in | Sh. J Prabhakar Ra | DIGP | 0863-2340152 | cybercrimes-cid@ap.gov.in |
| Sh. Jimmy Chiram | SP | 0360-2212471 | spcr@arunpol.nic.in, spsit@arunpol.nic.in | Sh. Take Ringu | DIGP | 0360-2215518 | sit@arunpol.nic.in |
| Sh. Debajit Hazarike | DIGP | 0361-2529840 | digp-cid@assampolice.gov.in | Sh. Surendra kuma | IGP | 0361-2524494 | igp-cid@assampolice.gov.in |
| Sh. D.Amarcase | ASP | 0612-2216236 | cybercell-bih@nic.in | Sh. Shiv Kumar Jha | DIG | 0612-2238098 | dig-bih@nic.in |
| Manisha Thakur R | AIGP | 0771-2511606 | aigtech-phq.cg@gov.in | Sh. R K Vij | SPL DGP | 0771-2511623 | vijrk@gov.in |
| Sh. Karthik Kashyap | SP | 0832-2443082 | picyber@goapolice.gov.in spcyber@goapolice.gov.in | Sh. Paramaditya | DIGP | 0832-2420883 | digpgoa@goapolice.gov.in |
| Sh. Rajesh GadhiyaSI | SPDSI | 079-23255545 | cc-cid@gujarat.gov.in | Sh. Ajay Tomar | ADGP | 079-23250798 | cc-cid@gujarat.gov.in |
| Sh. Ashwin Shenvi | SP | 01733-253023 | sp.crime2pkl@hry.nic.in | Sh. Kuldip Singh Si | ADGP | 01733-253230 | igp.crime2-hry@nic.in |
| Sh. Narveer Rathore | DSP | 0177-2621331 | polcyberps-shi-hp@nic.in | Sh. Sandeep Dhaw | SP | 0177-2627955 | sp-cybercr-hp@nic.in |
| Sh. Syed Ahfadul-ul-I | IGP | 0191-2572475 | igcrime@jkpolice.gov.in igcrime-jk@nic.in | Sh. B Srinivas | ADGP | 0191-2582996 | adgpcidjk@jkpolice.gov.in |
| Sh. Sunil BhaskarSh. | SPDSI | 0651-22100580651-2 | cyberps@jhpolice.gov.in | Sh. Ranjit Prasad | IGP | 0651-2490046 | ig-orgcid@jhpolice.gov.in |
| Sh. Chandra GuptaSh | SPDSI | 080-22094436 | spccpscid@ksp.gov.in ccps@kar.nic.in | Sh. T D Pawar | DIGP | 080-22251817 | digadmincod@ksp.gov.in |
| Sh. Sreejith | IGP | 0471-2319787 | igpcrimes.pol@kerala.gov.in cyberps.pol@kerala.gov.in | Sh. Dr. Shaik Darve | ADGP | 0471-2722215 | adgpcrimes.pol@kerala.gov.in |
| Sh. Niranjan B Vayanrg | DIGPA | 755-2443483 | mpcyberpolice@mppolice.gov.in aig1cybercell@mppolice.gov.in niranjan.vayangankar889@mppolice.gov.in | Smt. Aruna Mohan | SPL DGP | 0755-2770248 | spl.dgp-cybercell@mppolice.gov.in |
| Sh. Balsing Rajput | SP | 022-22160080 | sp.cbr-mah@gov.in control.cpaw-mah@gov.in apil .cpaw-mah@gov.in | Sh. Brijesh Singh | SPL IGPA | 022-22026672 | ig.cbr-mah@gov.in |
| Ms. Joyce Lalremmaw | SP | 0385-2451501 | cidcb-mn@nic.in cybercrime.mn@gov.in | Sh. Themthing Nga | DIGP | 0385-2450573 | themthing.ng@gov.in |
| Sh. R. Muthu | SP | 0364-2504416 | r.muthu@ips.gov.in ccw-meg@gov.in | Sh. F G Kharshiing | DIGP | 0364-2550141 | fg.kharshiing@ips.gov.in |
| Sh. Zosangliana | SP | 0389-2334082 | cidcrime-mz@nic.in | Sh. Balaji Srivastav | DGP | 0389-2334682 | polmizo@rediffmail.com |
| Ms. Sonia Singh | IGP | 0370-2242712 | cybercrimeps-ngl@gov.in | Sh. Renchamo P. K | ADGP | 0370-2223897 | renchamo.p@gov.in |
| Sh Anil Kumar Dash | ASP | 0671-2974401 | sp1cidcb.orpol@nic.in dirscrb.odpol@nic.in | Sh. Madkar Sandee | SP | 0671-2306071 | sp1cidcb.orpol@nic.in |
| Sh. Dhruman Harshar | AIG | 0172-2226258 | aigcc@punjabpolice.gov.in | Sh. Hardial Singh M | DIGP | 0172-2226258 | aigcc@punjabpolice.gov.in shocc@punjabpolice.gov.in |
| Sh. Pankaj Chaudhary | SP | 0141-2740169 | ccps-raj@nic.in | Sh. Sharat Kaviraj | DIGP | 0141-2740898 | sharat.kaviraj@rajasthan.gov.in |
| Sh. Prathap Pradhan | DIGP | 03592-20208703592 | spcid@sikkimpolice.nic.in | Sh. Sonam Detchu | DySP | 03592-204297 | spcid@sikkimpolice.nic.in |
| Ms. B Shamoondeswa | SP | 044-28512527 | spcybercbcid.tnpol@nic.in cbcyber@nic.in | Sh. C Sridhar | IGP | 022-28512503 | cbcyber@nic.in |
| Sh. Govind SinghSh. I | ADGP | 040-23242424 | adg_cid@tspolice.gov.in ccps.cid@tspolice.gov.in | Smt. Swathi Lakra | IGP | 040-23147604 | igp_wpc@cid.tspolice.gov.in |
| Ms.Saraswati R IPS | IPS | 0381-2304344 | spcybercrime@tripurapolice.nic.in | Sh. Subrata Chakra | AIGP | 0381-2304344 | aigcrime@tripurapolice.nic.in |
| Sh. Barinderjit Singh | SSP | 0135-2651689 | spstf-uk@nic.in ccps.deh@uttarakhandpolice.uk.gov.in | Sh. Deepam Seth | IGP | 0135-2712563 | dgc-police-ua@nic.in |
| Sh. Vivek Ranjan | DSP | 0522-2721690 | ccpsnoida@upstf.com | Dr. Kalluri SP Kuma | ADGP | 0522-2208598 | ccpsnoida@upstf.com |
| Sh. Rajesh Kumar Yao | DIGP | 033-24792955 | ccpwb@cidwestbengal.gov.in digcyber@cidwestbengal.gov.in | Sh. Ashok Kumar P | IGP | 033-24791830 | ig2@cidwestbengal.gov.in |
| Sh. Sanjay Kumar | IGP (A) | 03192-232334 | igpint.and@nic.in | Smti. Shalini Singh | IGP (L&O) | 03192-232244 | igplo.and@nic.in |
| Ms. Rashmi Sharma Y | DSP | 0172-2710046 | dspccic.chd@nic.in police-chd@nic.in | Ms. Nilambari Jagao | SSP | 0172-2760001 | ssput-chd@nic.in |
| Sh. Anyesh Roy | DCP | 011-23746615 | acp-cybercell-dl@nic.in acp.cybercell@delhipolice.gov.in | Sh. Prem Nath | ACP | 011-23490236 | jtcp-ops-dl@delhipolice.gov.in |
| Sh. Vipul Anekant | ASP | 0260-2254101 | sdpo-diu-dd@nic.in sebastian.devasia@gov.in | Sh. Vikramjit Singh | SP | 0260-2250942 | sp-dmn-dd@nic.in |
| Sh. Manasvi Jain | Dy. SP | 0260-2632888 | dysp-hq-dnh@gov.in / For correspondence - itcell-dnhp@mha.gov.in | Sh. Sharad B. Dara | SP | 0260-2643022 | sp-sil-dnh@nic.in |
| Sh. Mahesh kumar Ba | SSP | 0413-2224083 | cybercell-police.py@gov.in sspci.pon@nic.in | Sh. Dr. VJ Chandra | DIGP | 0413-2231386 | dig.pon@nic.in |
| Sh. Mayank Bansal | DSP | 04896-262367 | | Sh. Shibesh Singh | SSP | 04896-262258 | lak-sop@nic.in |

## *II. NCPCR*

Lodge complaints in person, by post, by messenger, or by any means to the following address:

National Commission for the Protection of Child Rights (NCPCR),
5th Floor, Chandralok Building, 36 Janpath,
New Delhi 110 001

## USEFUL RESOURCES

Cyber Security Awareness, MInistry of Electronics and Information Technology
https://infosecawareness.in/home/index.php

Government of India, Ministry of Home Affairs. A Handbook for Adolescents/Students on Cyber Security. https://m-ha.gov.in/sites/default/files/CyberSafety_English_Web_03122018_0.pdf

Being Safe Online: Guidelines for raising Awareness among children, parents, educators and the general public
https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=1637&lid=1661

http:// www.aarambhindia.org

## ***References***

https://home.crin.org/briefing-childrens-rights-in-the-digital-age
https://www.internetmatters.org/
https://infosecawareness.in/home/index.php
e-Raksha by Cyber Peace Foundation

Children's rights in the digital age adapted from Livingstone, S., and Bulger, M. (in press) A global research agenda for children's rights in the digital age. Journal of Children and Media.

**Visit Cyber Peace Resource Center for More Informative Contents and Videos**

https://www.cyberpeacecorps.in/CPCRC/

# Cyber Safety Booklet for Children