सत्यमेव जयते

NCPCR

Draft

GUIDELINES ON CYBER SAFETY

(for inclusion in)

MANUAL

ON

SAFETY AND SECURITY OF CHILDREN IN SCHOOLS

by

NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS

5th Floor, Chanderlok Building, 36 Janpath,
New Delhi 110001

2020-21

CYBER SAFETY

TABLE OF CONTENTS

INTRODUCTION

The Internet is without a doubt one of the best resources available to us. Information Technology has become one of the most important and integral part of our daily lives.
The 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.

In short, cyber safety means being secure online. The online environment is rife with threats to our safety and security. Naturally, we wish to mitigate these threats where possible, not only as an organization but also in our individual capacities. These threats are everything that can prove a risk, for example a publicly accessible internet connection, phishing emails, suspicious links, downloadable documents or apps[1]. Cyber safety helps to avoid those risks but also helps to protect against their consequences, because it is impossible to avoid all hazards. Even when someone complies with all customary security requirements, they could still become the target of an attack.

Children and young people have shown greater ability to adapt and to 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 mobilize 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.

---

[1]" Cybersafety: Cyber Safety" (*Universiteit Twente*) <https://www.utwente.nl/en/cyber-safety/cybersafety/> accessed December 30, 2020

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 marginalized 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.

Internet, the most interactive technological platform of this century, has become an integral part of our daily lives. It is a learning and communication tool that offers us a wide range of opportunities. It is an invaluable source of knowledge and encourages creativity and imagination.

Internet ethics involves our approach while using it for different purposes. We should be aware that we should always be honest and respect the rights and property of others on the web.

The ”Police” and ”Public Order” are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes including crimes related to exploitation of children; through their law enforcement machinery. The law enforcement agencies take legal action as per provisions of law against persons involved in digital sexual exploitation/ abuse of children. The Information Technology (IT) Act, 2000 has adequate provisions to deal with prevailing cyber-crimes. Section 67B of the Act specifically provides stringent punishment for publishing, browsing or transmitting child pornography in electronic form. Further, sections 354A and 354D of Indian Penal Code provide punishment for cyber bullying and cyber stalking against women.

Ministry of Home Affairs has approved a scheme namely ’Cyber Crime Prevention against Women and Children (CCPWC) ‘under which an online Cyber Crime reporting portal, (www.cybercrime.gov.in) has been launched to enable public to report complaints pertaining to Child Pornography/ Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. This portal facilitates the public to lodge complaints anonymously or through Report and track option. The Ministry of Women and Child Development had enacted the Protection of Children from Sexual Offences Act, 2012 (POCSO Act) as a special law to protect children from offences of sexual assault, sexual harassment and pornography. Section 13 to Section 15 deals with the issue of child pornography.

Section 14 and Section 15 lays down the punishment for using child for pornographic purposes and for storage of pornographic material involving child.

Further Section 28 of the POCSO Act 2012 provides for establishment of Special Courts for the purpose of providing speedy trial of offences under the Act.

Further, National Commission for Protection of Child Rights (NCPCR) and State Commission for Protection of Child Rights (SCPCRs) are also mandated to monitor the implementation of the POCSO Act, 2012.

The National Commission for Protection of Child Rights (NCPCR) was set up in March 2007 under the Commissions for Protection of Child Rights (CPCR) Act, 2005, an Act of Parliament (December 2005) under the administrative control of the Ministry of Women & Child

Development, Government of India. The NCPCR's Mandate is to ensure that all Laws, Policies, Programmes, and Administrative Mechanisms are in consonance with the Child Rights perspective as enshrined in the Constitution of India and as also under the UN Convention on the Rights of the Child. The Child is defined as a person in the 0 to 18 years age group.

NCPCR visualizes a rights-based perspective flowing into National Policies and Programmes, along with nuanced responses at the State, District and Block levels, taking care of specificity and strengths of each region.

CHECKLIST

S.No	LIST OF GUIDELINES TO BE COMPLIED WITH	YES/NO
1.	Whether the school have a document that defines procedures and policies that the school implements to safeguard against any online safety incident?	
2.	Whether the school have a document that defines procedures and policies that the school implements to safeguard in response to any online safety incident?	
3.	Whether the school have a special committee that implements the provisions under the guidelines regarding cyber safety?	
4.	Whether the school have any draft policy regarding actions to be taken against an accused of cyber- crime ?	
5.	Whether or not the school has any monitoring committee to track any kind of cyber- attack on children when at school?	
6.	Whether or not the school actively conducts programs which provides information regarding each category/kind of cyber threats?	
7.	Whether or not the school has a special redressal cell for a child victim of any kind of cyber- crime to help the child and parents to file a formal complaint with the authorities under the provisions of law.	
8.	Whether or not the school provides education regarding cyber crimes through various mediums to educate the child about what cyber-crimes are and what are the do's and don'ts that a child must keep in mind to ensure his/her safety?	

9.	Whether or not the school ensures supervision on children when they attend computer labs classes or any other classroom where they can become a victim of cyber-crime?	
10.	Whether or not the school have proper information as to which authorities cybercrime can be reported? Are School Authority and children oriented on procedures to be followed and steps prescribed within the legal framework in the event of cyber abuse or crime – legal recourse and information about Cyber Crime Department in the Police?	
11.	Whether or not children are taught/educated to keep their personal data and information secure to minimize the risks of cyber crime ?	
12.	Whether or not the staff of the school is formally trained for e-safety?	
13.	Does the school have any drafted policy on misuse of technology/equipment's by pupils and staff ?	
14.	Does the school have any policy on monitoring the usage of camera's including webcams, the use of video conferencing equipment, mobile phones etc. by the staff or children to ensure safety of children.	

2

CYBER SAFETY AND ITS IMPORTANCE

Internet, computers, smart phones and other communication technology devices have become an integral part of our lives. Cyber crimes can be defined as offences that maybe committed against individuals or against the companies or institutions by use of computers, internet or mobile technology.

Cybercrime offences can be committed by cybercriminals by using of platforms like social networking sites, emails, chat rooms, websites etc to attack its victims. This offence is not just limited to adults, but also children can be a prey to the offence.[2]

Cyber safety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful to other people online, and using good Internet etiquette.[3] It includes body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Since information infrastructure and Internet became bigger and more complex, it is now even more critical to maintain systems functional and alert to security issues. Though the system administration tasks have become easier in recent years, school administrators need to be more updated on the systems and network security In recent years, all systems are exposed to Internet; hence there is increased challenge in maintaining and protecting them from the attackers.

Schools play a key role in promoting internet safety. Schools are primarily responsible for keeping systems, computers, network devices secure and functional. It is important to keep the information as secure as we keep the systems and network devices in the organisation.

---

[2] GOVERNMENT OF INDIA, MINISTRY OF HOME AFFAIRS. (2020). A HANDBOOK FOR ADOLESCENTS/STUDENTS ON CYBER SAFETY. Retrieved 2O2O, from https://www.mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf

[3] Be safe in Cyber World. (n.d.). Retrieved from https://ncert.nic.in/pdf/notice/cyber_safety_security.pdf

Cyber safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviours protect personal information and reputation and include safe practices to minimize danger online.

3

CYBER SECURITY

The dictionary meaning says that Cyber Security is state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. It is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user‘s assets. Organization and user‘s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cyber security ensures the maintenance of the security properties of the organization and user‘s assets against security risks in the networked environments. It is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.[4]

3.1 Elements of cyber security include:

1.Application security which comprises of software, hardware, and procedural methods to protect applications from external threats.

2.Information security is the practice of avoiding information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. IT Security and Information assurance are two major aspects of information security.

[4] T.P, D., Assistant Prof. (2018). *Survey on need for Cyber Security in India* (pp. 2-3). Bangalore, Karnataka: Acharya Institute of Technology.

3.Network security which consists of the provisions and policies adopted by a network administrator. They prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or any other authenticating information that allows them to access information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, Government agencies and individuals.

4. End-user education involves educating end users with various information attacks and how to avoid them. For example, while registering password, tell end user what should be the length and characteristics of complex password. Provide suitable education about what are the precautions they have to take to avoid cyber crimes. Also, sometimes actions to be taken in case if they are victim.

3.2 Challenges in Cyber Security

Cyber security has been considered as one of the most urgent national security problems. Cyber security must address not only deliberate attacks, from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize a network in unpredictable ways.

The defense of cyberspace necessarily involves the forging of effective partnerships between the public organizations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like Government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The defense of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

4

COMMON THREATS IN CYBER SAFETY

4.1 PHISHING

Phishing is a type of social engineering attack often used to steal data, including login credentials and credit card numbers. Phishing occurs when attackers/scam artists masquerading as a trusted entity send text, email, or pop-up messages to get people to share their personal and financial information. The recipient is then tricked into clicking a malicious link which can lead to the installation of malware, the freezing of system as part of a ransom ware attack or revealing of sensitive information. The attackers often use such sensitive information to commit identity theft. [5]

How One Can Avoid Phishing :

- One must **not reply** to any text, email, or pop-up messages that ask for personal or financial information, and further one must not click any links in the message. A person should resist the urge to cut and paste a link from the message into their web browser. For example, if a person wants to check for their financial account, then they must only use authorized source like typing in the web address from your billing statement or check one's banking details.
- One **must not give any personal information** on the phone in response to a text message. Some scammers send text messages that appear to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." If you give them your information, they use it to run up charges in your name.

[5]STOP. THINK. CONNECT. ™ Toolkit. (n.d.). Retrieved December 30, 2020, from https://www.cisa.gov/publication/stop-think-connect-toolkit

- A person must **Be cautious** about opening any attachment or downloading any files from emails that one receives, regardless of who sent them. Unexpected files may contain viruses or spyware that the sender doesn‘t even know are there.
- **Use security software**, and update it regularly.
- **Read your mail**; review credit card and bank account statements as soon as you get them to check for unauthorized charges.
- Parents and Teachers must also **engage children** in activities creating awareness regarding phishing, so they can develop good Internet security habits at a very early stage. Parents & Teachers must lookout for ”teachable moments”—For example children must be shown various examples of phishing message, so as to help them understand that messages on the Internet aren‘t always what they seem.

4.2 CYBER BULLYING

Cyberbullying is bullying with use of digital technologies. It is a form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone , laptop, etc.[6] It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is a repeated behaviour, aimed at scaring, angering or shaming those who are targeted. For example :

- spreading lies about or posting embarrassing photos of someone on social media
- sending hurtful messages or threats via messaging platforms
- impersonating someone and sending mean messages to others on their behalf.

Face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying always leaves a digital footprint i.e a record that can prove useful and provide evidence to help stop the abuse.

[6] Government Of India, Ministry Of Home Affairs. (2020). A Handbook For Adolescents/Students On Cyber Safety. Retrieved 2O2O, from https://www.mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf

Protecting Oneself From Becoming A Victim Of Cyber Bullying:

Children should be educated to not accept friend requests from unknown people on social media platforms. They should be informed that:

i. Cyber bully/attacker can even create a fake account to befriend victims. As a thumb rule, add only those people online whom you know offline.

ii. Educate as to not share personal information like D.O.B, Address and phone number on social media or other platforms. One should be informed and educated as to one should always change privacy setting on social media platforms as to select who can access your posts online.

iii. One must be made aware of the importance of being careful and of not sharing phone number or any personal details in comments or posts on social media platforms.

iv. One must be made aware as to **Never install** unwanted software or apps like dating app, online games etc from unknown sources.

v. Educate that, If one feels hurt after reading a post from a friend or a stranger, one must not react aggressively. It may encourage the bully to keep posting such messages. If hurtful post/message is from a friend one should always request him or her to not to do it again. If one is repeatedly getting such messages/post, one must immediately inform parents or elders or guardians or teachers immediately so that one can get immediate support .

vi. Also, it is important to understand that one person can sometimes also become a cyberbully unintentionally, hence it is very important to remember that as a good netizen one should never share mean comments or hurtful messages pictures/videos online publicly or privately.

What can one do if they are a victim of cyber bullying ?

1. **One must Inform** parents/elders/guardians immediately.If cyberbullying happens in school, students must inform the Teacher immediately.

2. Identify the bully.

3. Block the bully.

4. Collect and save posts/messages.

5. Never respond to a bully aggressively.

4.3 CYBER GROOMING

Cyber grooming is defined as the process of ’befriending ‘a young person online to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse.

Cyber grooming is when someone (often an adult) befriends a child online and builds an emotional connection with future intentions of sexual abuse, sexual exploitation or trafficking. The main goals of cyber grooming are: to gain trust from the child, to obtain intimate and personal data from the child (often sexual in nature such as sexual conversations, pictures, or videos) in order to threaten and blackmail for further inappropriate material.[7]

Perpetrators often take on fake identities of a child or teen and approach their victims in child-friendly websites, leaving children vulnerable and unaware of the fact that they have been approached for purposes of cyber grooming. Conversations often start with inconspicuous and general questions about age, hobbies, school, family and progress into questions regarding sexual experience, with groomers convincing an exchange of erotic materials. However, the child or teen can also unknowingly initiate the grooming process when they partake in websites or forums with lucrative offers such as money in exchange for contact details or intimate photos of themselves.

The cyber grooming process itself can happen quickly, however the negative impact on the victim can be long-term. In addition to feeling violated and betrayed, a child who has been groomed may feel responsible for or for deserving the abuse, leading to self-blame and low self-esteem. Thus, it is crucial not only to raise awareness about the dangers of cyber grooming and

[7] (n.d.). Retrieved December 30, 2020, from https://bellevueparkss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Parent information/cyber-safety-and-security-guide

safe practices of internet technologies but also for international legislations to criminalize all types of child grooming. Cyber grooming is often considered to be a gateway to more serious offences of sexual exploitation of children.

Protecting Oneself/Child from becoming a victim of cyber grooming:

1. One must be educated as to not accept friend request from unknown people on social media platforms. Cyber groomer can even create a fake account to befriend victims.

2. One must be educated as to not share their personal information like date of birth, address, phone number and school name on social media or other online platforms. One can go to the privacy settings on their social media platforms as to select who can access their posts online. One must try to restrict access of their profile to their friends only.

3. One must always be cautious when the person one is chatting to give too many compliments regarding their appearance in just a short span of your acquaintance.

4. One must Avoid talking to people who ask questions related to one's physical or sexual experiences . One can either ask the person to stop asking such questions when it makes one feel uncomfortable. If they continue to do the same, one must immediately inform parents/elders/teachers etc.

5. One must Educate people to not talk to people who asks to share their sexually explicit photographs or videos.

6. Educate children to never turn on webcam for any unknown person.

7. Educate a child to talk to their elders or parents, if their chat partner suggests to keep their conversation with them secret.

8. Educate a child as to not go and meet any person whom they met online alone. One must always take a friend or any elder person while going to meet someone whom one met online.

9. One must be educated/made aware to never install unwanted software and apps like dating app, online games etc from unknown sources. One should be very careful while chatting in the chat rooms. One should never share personal details in the chat room and limit their identity.

What can one do if they are a victim of cyber grooming ?

A. Inform parents/elders immediately. Inform Teacher/Head of the institution if incident occurs in school.

B. Block the groomer/attacker.

C. One must collect and save messages.

D. Elders/parents must be made aware so they can contact local police station to lodge a complaint against the groomer.

4.4. GAMING

Online gaming can be a fun way for kids to connect with others, but it's important for them to understand the risks and have the desired knowledge and awareness as how to handle certain situations. For example, kids should avoid posting pictures of themselves or releasing any other personal information to their fellow gamers and must know what to do if another player starts harassing them.[8]

The Entertainment Software Rating Board, which assigns the familiar age and content ratings for video games and mobile apps, gives a breakdown of the various types of games:

1. **Boxed games**: Games that come on a disc or cartridge that are purchased from a store or online and played on a game device like a console, handheld or PC.

[8] (n.d.). Retrieved December 30, 2020, from https://bellevueparkss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Parent information/cyber-safety-and-security-guide

2. **Digital download**: These are downloaded directly to the console, PC or handheld device. Most consoles (Xbox 360, PlayStation 3 and Wii) have their own online marketplaces where games can be downloaded. Some are full-length feature titles while many others are more casual in nature, like puzzle and word games.

3. **Mobile storefronts:** Smartphones and tablets let users download apps from online marketplaces linked to a credit card, e-wallet or your mobile phone account. Games are the most popular category of mobile apps. Like all games, their content can vary in terms of age-appropriateness.

4. **Subscription**: Online games or arcades in which players sign up for accounts that let them play games for set amounts of time and fees. Subscription services typically eliminate the need to physically possess a game at all by streaming the gameplay experience right to the device or accessing it from the service‘s own servers (or cloud gaming).

5. **”Free-to-play” and ”freemium”**: These games are typically supported by ads instead of purchase or subscription fees; a ”freemium” game lets you play a limited portion for free but requires that you pay to access new content or features. Mobile apps, browser-based games and other types of casual games will often use these business models.

6. **Social networking games**: Played from within a social network like Facebook, these games encourage users to share content and updates with others in their social network. These games often include the opportunity to buy in-game items with real money, reward players for recruiting their friends to join the game and may leverage some of a user‘s personal information (included in their social media profile) to tailor the game experience or advertisements to their interests.

How can one protect themselves?

1. Educate children as to not share their personal information like name, D.O.B, address and phone number with players while playing online games. One doesn’t know or is aware as to who the players are and what are their intention? One may end up sharing their information with scammers or cyber bullies.

2. Educate children to never share their or their parents credit card/debit card details with anyone when they are playing online games. Some cyber criminals befriend children by helping them winning games or sharing points.

3. Educate to 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. One may end up downloading viruses and malware which can compromise security of their computer's or smart phone.

4. Always install a good anti-virus software on one's computer, smartphone, or handheld devices. Regularly update the anti-virus and other applications.

5. Never share passwords with anyone. One should use a complex password for their online gaming account and other online accounts. It is a good practice to change passwords on regular interval.

6. Never use voice chat or webcam while playing online games.This may share one's identity with other players and attract cyber bullies and other cyber criminals.

7. Educate children to never meet in person with someone from one's online gaming world.

8. If anyone face any challenge in online gaming world, one must immediately inform their parents or elders so that they one can gain immediate support and guidance.

5

LAWS RELATED TO CYBER SAFETY

"Police" and "Public Order" are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation, and prosecution of crimes including crimes related to exploitation of children, through their law enforcement machinery. The law enforcement agencies take legal action as per provisions of law against persons involved in digital sexual exploitation/ abuse of children.

Cyber Crimes under IT Act, 2000, Section 67B of the Act specifically provides stringent punishment for publishing[9], browsing or transmitting child pornography in electronic form. Further, sections 354A and 354D of Indian Penal Code provide punishment for cyber bullying[10] and cyber stalking against women[11].

Some of the Laws related to cyber-crime are stated below ((The legal provisions shall be applicable along with relevant provisions of POCSO Act, 2012 and its subsequent Amendments):

1. **Child Pornography**

There is no legal definition in the Indian Legislation, Child pornography is defined as the representation of a child engaged in real or simulated sexual activities.

This includes the circulation through any form of media (video, picture, sound recording) viathe internet through a computer, telephone, mobile or tablet.

Children can be enticed and groomed into engaging in sexual activity, whichdocumented and dist ributed for personal or commercial consumption on the internet.

In India, any sexual act performed with a child, whether consensual or otherwise,

is a criminal offence. For example, if a person engages in sexual intercourse with a child and records the act, the perpetrator of such activity could be charged with rape under the Section 376 IPC and Section 4 of POCSO along with specific sections that address Child pornography.

Applicable Legal Provisions

- **Section 11(v) and (vi) Protection of Children from Sexual Offences (POCSO) Act, 2012**

Sexual harassment- A person is said to commit sexual harassment upon a child when such person with sexual intent,—

(i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or

[9] IT ACT 2000, s 67B
[10] Indian Penal Code, s 354A
[11] Indian Penal Code 1860, s 354D

(ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or

(iii) shows any object to a child in any form or media for pornographic purposes; or

(iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or

(v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or

(vi) entices a child for pornographic purposes or gives gratification therefor.

- **Section 13, 14, 15 POCSO ACT, 2012**

Use of Child for pornographic purposes - Whoever, uses a child in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes[12]-

(a) representation of the sexual organs of a child;

(b) usage of a child engaged in real or simulated sexual acts (with or without penetration);

(c) the indecent or obscene representation of a child, shall be guilty of the offence of using a child for pornographic purposes.

Punishment for using child for pornographic purposes—

(1) Whoever uses a child or children for pornographic purposes shall be punished with imprisonment of either description which may extend to five years and shall also be liable to fine and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also be liable to fine.

(2) If the person using the child for pornographic purposes commits an offence referred to in section 3, by directly participating in pornographic acts, he shall be punished with

[12] POCSO Act 2012, s13

imprisonment of either description for a term which shall not be less than ten years but which may extend to imprisonment for life, and shall also be liable to fine.

(3) If the person using the child for pornographic purposes commits an offence referred to in section 5, by directly participating in pornographic acts, he shall be punished with rigorous imprisonment for life and shall also be liable to fine.

(4) If the person using the child for pornographic purposes commits an offence referred to in section 7, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than six years but which may extend to eight years, and shall also be liable to fine.

(5) If the person using the child for pornographic purposes commits an offence referred to in section 9, by directly participating in pornographic acts, he shall be punished with imprisonment of either description for a term which shall not be less than eight years but which may extend to ten years, and shall also be liable to fine.[13]

Punishment for storage of pornographic material involving child - Any person, who stores, for commercial purposes any pornographic material in any form involving a child shall be punished with imprisonment of either description which may extend to three years or with fine or with both.[14]

- **Section 66E Information Technology (IT) Act,2000**

Violation of privacy

Section 66E of I.T. Act provides punishment for violation of privacy. Whoever intentionally or knowingly captures or publishes or transmits the images of a private area of any person without his or her consent in which violates the privacy of that person is punishable with imprisonment which may extend upto three years with fine not exceeding rupees two lakh or with both.[15]

[13] POCSO Act,2012 s 14
[14] POCSO Act s 15
[15] IT Act,2000 s 66E

- **Section 67, IT Act,2000**

Punishment for publishing or transmitting obscene material in electronic form-Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.[16]

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form - Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.[17]

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.–Whoever,–

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

[16] IT Act,2000 s67
[17] IT Act 2000, s 67 A

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes. Explanation–For the purposes of this section, "children" means a person who has not completed the age of 18 years[18]

Section 292 Indian Penal Code, (IPC), 1860

Sale, etc., of obscene books, etc.

1*[292. Sale, etc., of obscene books, etc.

2*[(1) For the purposes of sub-section (2), a book, pamphlet, paper, writing, drawing, painting representation, figure or any other object, shall be deemed to be obscene if it is lascivious or appeals to the prurient interest or if its effect, or (where it comprises two or more distinct items) the effect of any one of its items, is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.]

[18] IT Act 2000, s 67B

3*[(2)] Whoever-

(a) sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, reduces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever, or

(b) imports, exports or conveys any obscene object for any of the purposes aforesaid, or knowing or having reason to believe that such object will be sold, let to hire, distributed or-publicly exhibited or in any manner put into circulation, or

(c) takes part in or receives profits from any business in the course of which he knows or has reason to believe that any such obscene objects are, for any of the purposes aforesaid, made, produced, purchased, kept, imported, exported, conveyed, publicly exhibited or in any manner put into circulation, or

(d) advertises or makes known by any means whatsoever that any person is engaged or is ready to engage in any act which is an offence under this section, or that any such obscene object can be procured from or through any person, or

(e) offers or attempts to do any act which is an offence under this section, shall be punished 1 [on first conviction with imprisonment of either description for a term which may extend to two years, and with fine which may extend to two thousand rupees, and, in the event of a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and also with fine which may extend to five thousand rupees].

2*[Exception-This section does not extend to-

(a) any book, pamphlet, paper, writing, drawing, painting, representation or figure- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern, or

(ii) which is kept or used bona fide for religious purposes;

(b) any representation sculptured, engraved, painted or otherwise represented on or in-

(i) any ancient monument within the meaning of the Ancient Monuments and Archaeological Sites and Remains Act, 1958 (24 of 1958), or

(ii) any temple, or on any car used for the conveyance of idols, or kept or used for any religious purpose.]] [19]

Section 354A(iii) and 354C IPC, 1860

Sexual harassment and punishment for sexual harassment-

1. A man committing any of the following acts—

i. physical contact and advances involving unwelcome and explicit sexual overtures; or
ii. a demand or request for sexual favours; or
iii. showing pornography against the will of a woman; or
iv. making sexually coloured remarks, shall be guilty of the offence of sexual harassment.

Any man who commits the offence specified in clause (i) or clause (ii) or clause (iii) of sub-section (1) shall be punished with rigorous imprisonment for a term which may extend to three years, or with fine, or with both.

Any man who commits the offence specified in clause (iv) of sub-section (1) shall be punished with imprisonment of either description for a term which may extend to one year, or with fine, or with both.[20]

Section 354C- Voyeurism

Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image[1] shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either

[19] IPC 1860, s 292
[20] IPC 1860, s 354A

description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.[21]

2. Cyber stalking

Cyberstalking is generally defined as the use of internet or any other electronic means to stalk and harass an individual, group or organization. A child is said to be cyberstalked when he/she is repeatedly or constantly followed, watched or contacted through any electronic means. The movement of the child is tracked and privacy is invaded.

Applicable Legal Provisions

Section 11(iv) POCSO Act, 2012

Sexual harassment- A person is said to commit sexual harassment upon a child when such person with sexual intent,[22]—

(i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or

(ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or

(iii) shows any object to a child in any form or media for pornographic purposes; or

(iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or

(v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or

(vi) entices a child for pornographic purposes or gives gratification therefor.

Section 354D IPC,1860

[21] IPC 1860,s 354C
[22] POCSO Act 2012, s 11(iv)

(1) Any man who—

1. follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
2. monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking;

Provided that such conduct shall not amount to stalking if the man who pursued it proves that—

1. it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or
2. it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or
3. in the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.[23]

Section 509 IPC,1860

Word, gesture or act intended to insult the modesty of a woman

Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to three years, and also with fine[24].

3. Cyber Bullying

[23] IPC 1860, s 354D
[24] IPC 1860,s 509

"Bullying" is defined as harassing someone with unwanted and repeated written, verbal or physical behaviour. It also involves the use of intimidate, threat or insult to another person.

Cyberbullying is a form of criminal intimidation as the intention is to put another person under threat.

Applicable Legal Provisions

Section 503,506,507 IPC,1860

Criminal Intimidation

Whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, commits criminal intimidation.[25]

Punishment for Criminal Intimidation

Whoever commits the offence of criminal intimidation shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both;
If threat be to cause death or grievous hurt, etc and if the threat be to cause death or grievous hurt, or to cause the destruction of any property by fire, or to cause an offence punishable with death or imprisonment for life, of with imprisonment for a term which may extend to seven years, or to impute unchastity to a woman, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.[26]

Criminal Intimidation by an Anonymous Communication

Whoever commits the offence of criminal intimidation by an anonymous communication, or having taken precaution to conceal the name or abode of the person from whom the threat comes, shall be punished with imprisonment of either description for a term which may extend to two years, in addition to the punishment provided for the offence by the last preceding section.

[25] IPC 1860, S 503
[26] IPC 1860, s 506

4. Grooming

Grooming refers to the process of establishing an emotional connection with a child by gaining his/her trust, with the intention of exploiting the child at later stage. In grooming, the resulting exploitation is usually sexual in nature such as creating child pornographic content or sexual abuse.

Applicable Legal Provisions

Section 11 (vi) POCSO Act, 2012

Sexual harassment- A person is said to commit sexual harassment upon a child when such person with sexual intent,—

(i) utters any word or makes any sound, or makes any gesture or exhibits any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or

(ii) makes a child exhibit his body or any part of his body so as it is seen by such person or any other person; or

(iii) shows any object to a child in any form or media for pornographic purposes; or

(iv) repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital or any other means; or

(v) threatens to use, in any form of media, a real or fabricated depiction through electronic, film or digital or any other mode, of any part of the body of the child or the involvement of the child in a sexual act; or

(vi) entices a child for pornographic purposes or gives gratification therefor.

Section 67 B (c) IT Act

Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.–Whoever,–

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes. Explanation–For the purposes of this section, "children" means a person who has not completed the age of 18 years.[27]

5. Hacking

While' hacking' is not legally defined, the components of this cybercrime are covered in Indian legislation under the IT Act. Hacking means dishonestly or fraudulently accessing a computer system/ device without the permission of the owner with the intention to steal, copy, alter, destroy any data therein or cause destruction to such system.

Applicable Legal Provisions

[27] IT Act 2000, s 67B (c)

Section 43 IT Act, 2000

[Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) Accesses or secures access to such computer, computer system or computer network [or computer resource];

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there-under;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

[(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

[he shall be liable to pay damages by way of compensation to the person so affected.][28]

[28] IT ACT 2000, s 43

Section 66 IT Act, 2000

Computer related offences - According to Section 66 of IT. Act, if any person dishonestly or fraudulently does any act mentioned in section 43, such person is punishable with imprisonment for a term which may extend upto three years or with fine which may extend upto rupees five lakhs or both.[29]

6. Identity Theft

Identity theft can be defined s when someone wrongfully obtains and or uses another person deceptively of fraudulently for an illegal purpose such as an economic gain or sexual abuse.

Section 66C IT Act, 2000

Punishment for Identity theft - Section 66C deals with punishment for identity theft. Any person who fraudulently or dishonestly makes use of electronic signature, password or other unique identification feature of any person is punishable with imprisonment for a term which may extend upto three years and fine which may extend upto rupees one lakh.[30]

7. Online Child Trafficking

Child trafficking is defined as the ”recruitment, transportation, transfer, harbouring or receipt” of a child for the purpose of exploitation. This definition comes from the United Nations Palermo Protocol, which has been adopted by Sweden and the majority of countries around the world, making it the internationally accepted definition of human trafficking. A child is defined by the Palermo Protocol and the United Nations Convention on the Rights of the Child (CRC) as any person under the age of 18.

Applicable Legal Provisions

Section 5 Immoral Traffic Prevention Act (ITPA),1956

Procuring, inducing or taking person for the sake of prostitution-

(1) any person who

[29] IT ACT 2000, s 66
[30] IT ACT 2000,s66C

(a) procures or attempts to procure a person, whether with or without his consent, for the purpose of prostitution; or

(b) induces a person to go from any place, with the intent that he may for the purpose of prostitution become the inmate of, or frequent, a brothel; or

(c) takes or attempts to take a person, or causes a person to be taken, from one place to another with a view to his carrying on, or being brought up to carry on prostitution; or

(d) causes or induces a person to carry on prostitution;

shall be punishable on conviction with rigorous imprisonment for a term of not less than three years and not more than seven years and also with fine which may extend to two thousand rupees and if any offence under this sub-section is committed against the will of any person, the punishment of imprisonment for a term of seven years shall extend to imprisonment for a term of fourteen years:

Provided that if the person in respect of whom an offence committed under this sub-section,

(i) is a child, the punishment provided under this sub-section shall extend to rigorous imprisonment for a term of not less than seven years but may extend to life; and

(ii) is a minor, the punishment provided under this sub-section shall extend to rigorous imprisonment for a term of not less than seven years and not more than fourteen years; * * * * *

(3) An offence under this section shall be triable-

(a) in the place from which a person is procured, induced to go, taken or caused to be taken or from which an attempt to procure or take such person is made; or

(b) in the place to which he may have gone as a result of the inducement or to which he is taken or caused to be taken or an attempt to take him is made.

Section 366(A) IPC,1860

Procuration of Minor Girl- Whoever, by any means whatsoever, induces any minor girl under the age of eighteen years to go from any place or to do any act with intent that such girl may be, or knowing that it is likely that she will be, forced or seduced to illicit intercourse with another

person shall be punishable with imprisonment which may extend to ten years, and shall also be liable to fine.[31]

6

REFERENCES

1. INDIAN PENAL CODE 1860
2. POCSO ACT,2012
3. IT ACT 2000
4. CBSE Guidelines On Cyber Safety
5. CERT Guidelines On Cyber Safety
6. Cyber Safety For Secondary And Senior Secondary Schools
7. MHA Cyber Safety Handbook Guidelines
8. Pragyata Guidelines For Digital Education
9. https://bellevueparkss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Parent information/cyber-safety-and-security-guide
10. STOP. THINK. CONNECT. ™ Toolkit. (n.d.). Retrieved December 30, 2020, from https://www.cisa.gov/publication/stop-think-connect-toolkit

[31] IPC 1860, S366A