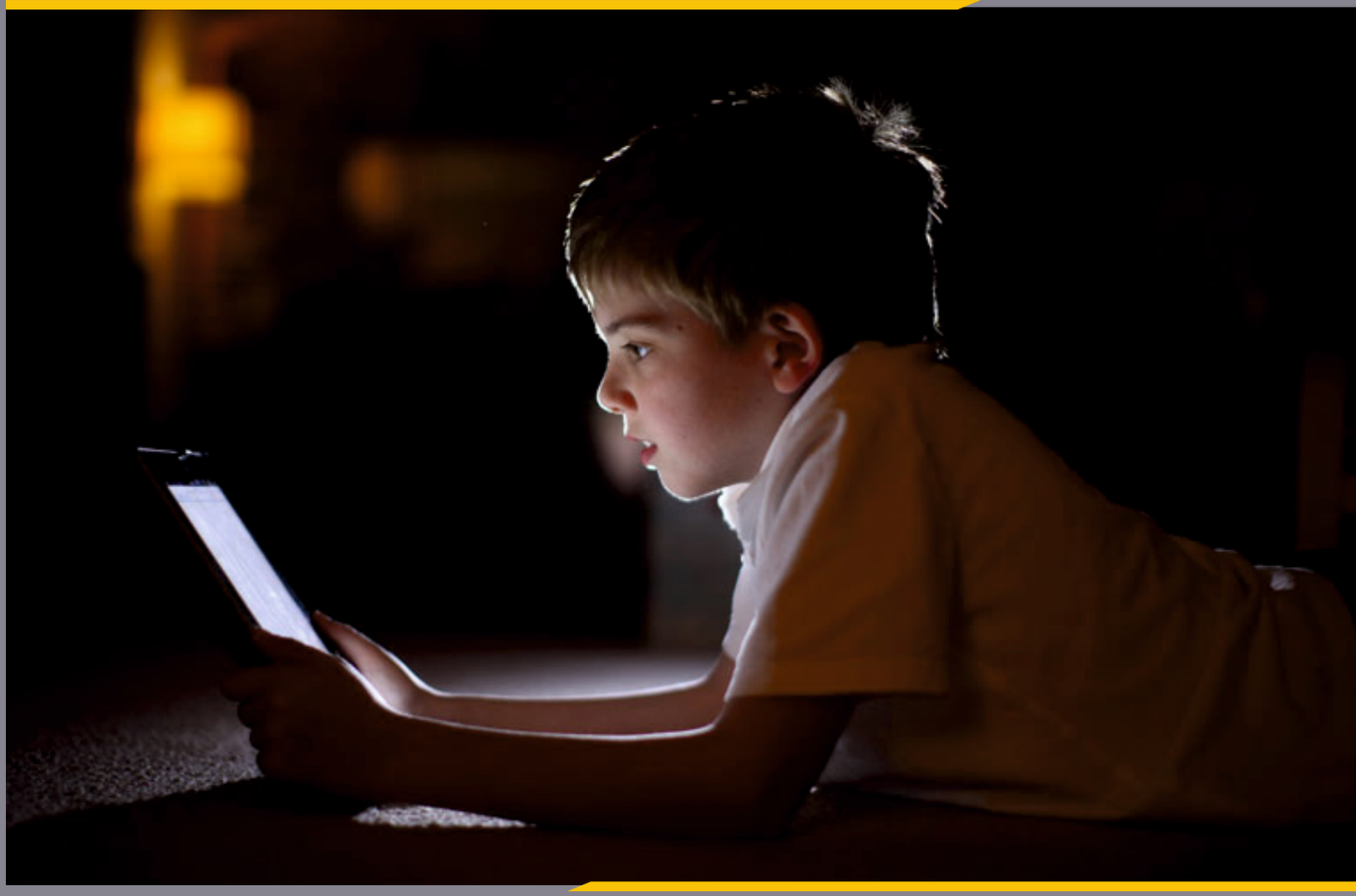
सत्यमेव जयते

Being Safe Online

Guideline for raising awareness among children, parents, educators and general public



NCPCR

National Commission for Protection of Child Rights (NCPCR)

Being Safe Online

Guideline and standard content for raising awareness among children, parents, educators and general public

National Commission for the Protection of Child Rights
5th floor, Chandralok Building, 36 Janpath,
New Delhi 110001

सत्यमेव जयते

स्तुति कक्कड़
Stuti Kacker
अध्यक्ष
Chairperson

भारत सरकार
GOVERNMENT OF INDIA
राष्ट्रीय बाल अधिकार संरक्षण आयोग
NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS
नई दिल्ली-110 001
New Delhi - 110 001

NCPCR

FOREWORD

India has the largest child population in the world. As per the 2011Census of India, there are 472 million children below the age of eighteen including 225 million girls. They constitute 39% of our population.

There is a growing concern regarding Child Online Safety. After many consultations, a need was felt to formulate guidelines and standard content for informing children, parents, educators and general public regarding online safety of children.

This Handbook on **"Being Safe Online - Guideline and standard content for raising awareness among children, parents, educators and general public'** is another major initiative taken by the Commission. The Handbook is intended to provide useful information on digital safety for children and is expected to serve a useful guide for all stakeholders especially children, parents and teachers etc.

We acknowledge the efforts of Ms. Karuna Bishnoi and Ms. Neelam Singh, Independent Child Rights, Policy and Development Professionals who have drafted this easy to read information on digital safety.

NCPCR would be happy to receive the valuable suggestions for updating and improving next edition of this Handbook.

(Stuti Kacker)
14th December 2017

5वां तल, चन्द्रलोक बिल्डिंग, 36, जनपथ, नई दिल्ली-110 001
5th Floor, Chanderlok Building, 36, Janpath, New Delhi-110 001
दूरभाष / Ph. : 011-23478212, 23731583 फैक्स / Fax : 011-23731584
ई-मेल / E-mail : cp.ncpcr@nic.in वेब / Web : www.ncpcr.gov.in

यशवंत जैन
Yashwant Jain
सदस्य
Member

सत्यमेव जयते

भारत सरकार
GOVERNMENT OF INDIA
राष्ट्रीय बाल अधिकार संरक्षण आयोग
NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS
नई दिल्ली-110 001
New Delhi - 110 001

NCPCR

ACKNOWLEDGEMENT

Cybercrime is a global phenomenon with a criminals acting at a transnational level. Cyber space is also being mi-used for child abuse which is increasing day by day both online and offline.

The National Commission for Protection of Child Rights (NCPCR) has been taking various steps for child online as well as offline safety in the country.

To overcome the challenges of cybercrime targeting children, NCPCR organized consultation in the month of December 2016, February 2017 and May 2017, wherein it was felt necessary that information for raising awareness and education for the digital safety of children (both Online and Offline) needs to be developed for the use of stakeholders to enable them to protect children from falling prey to cybercrime.

The NCPCR is grateful to UNICEF for producing a status report on Online Safety of Children. This report catalyzed our efforts. NCPCR's POCSO e-box has also been opened for cybercrime issues. All Cyber Crime Cells in the country have also been associated with it for quick grievance redressal.

I express my sincere gratitude to Ms. Stuti Kacker, Chairperson, National Commission for Protection of Child Rights (NCPCR), for her guidance and support.

I convey my thanks to my colleagues Smt. Rupa Kapoor, Member Child Health and Nutrition, Shri Priyank Kanoongo, Member Education, Smt. Geeta Narayan, Member Secretary, Shri Kulbir Krishan, Advisor (JJ & POCSO), Dr. Dhani Ram, Senior Consultant (JJ & POCSO), Shri Raman Gaur, Sr. Consultant and Ms. Nidhi Sharma, Consultant (Legal) for their valuable contributions.

(Yashwant Jain)
14th December 2017

द्वितीय तल, चन्द्रलोक बिल्डिंग, 36, जनपथ, नई दिल्ली-110 001
2nd Floor, Chanderlok Building, 36, Janpath, New Delhi-110 001
दूरभाष / Ph. : 011-23478261 फैक्स / Fax : 011-23724028
ई-मेल / E-mail : yashwant.ncpcr@gov.in
Web : www.ncpcr.gov.in Lodge your complaint at : www.ebaalnidan.nic.in

Table of Contents

1. INTRODUCTION

The National Commission for the Protection of Child Rights (NCPCR) has developed this guideline in view of the urgent need of mass awareness among various stakeholders i.e., children, parents, educationists and the general public about the potential risks and threats to children from the widespread and expanding use of technology in all aspects of day to day life - educational, social, work and financial. Since technology has become and will increasingly become an integral part of our lives, it is necessary that children and those concerned with their protection are aware of the potential risks and harms and can prevent such harm through timely safeguards, responsible and informed use of technologies, and know where and from whom to seek assistance, if necessary.

Based on children's rights based framework, this guideline provides the bare minimum standard content requirements for raising public awareness. It is, however, acknowledged that the information needs to be tailored for different audiences according to their profile (e.g., age, gender, location, and special circumstances), envisaged roles and expected responsibilities.

The principles outlined in the guideline should inform the initiatives for awareness and capacity development in the interests of child online safety. The framework and basic content may be used to devise and disseminate age and audience appropriate information. Some additional resources are listed in the annexures. The creative rendition and format have not been looked into as it is expected that individual agencies venturing into awareness creation initiatives will devise the format according to their area of work and target audience.

Ensuring accurate information through several channels that are commonly used by stakeholders, particularly children and young people, is critical for enabling responsible use of technology rather than control mechanisms, albeit selective supervision and oversight and guidance by concerned adults is desirable. For messages to be relevant for children and young people, agencies need to design communication and information materials and employ channels of communication based on a nuanced understanding of their communication and behavioral patterns. The importance of privacy and confidentiality should be negotiated and integrated within all educational initiatives considering the preferred channels of information through peers by this age group and the apprehensions regarding curtailment of their use of available technologies by the adults.

The chances of success of efforts to raise public awareness on any issue are increased if the environment within which the communicator(s) and audience(s) are located is conducive. The messages need to connect with the audience(s) if they are to take action. The desired changes can however occur only when the audience(s) are able to act upon the acquired knowledge and skills.

The major challenge for the group that collated this draft was the limited avenues for the audience(s) to apply the information that they are expected to receive. Reporting and seeking help in the interests of child online safety are seriously constrained by grossly inadequate reporting channels and lack of basic services. Who should the victims approach? What kind of service would be available to them? Who will serve them? Such questions need answers and follow-up with concrete actions. Otherwise, increased awareness cannot be expected to translate into positive results for children.

The following are some recommendations for strengthening the context within which public

awareness can effectively enhance online security for children. Increased awareness among the users can produce effective results in terms of strengthening the protective environment for children if the following conditions are met:

- **Comprehensive network for complaints redress:** The existing ChildLine 1098 network should be empowered to handle complaints and counsel children for addressing their problems and effectively connect with school counsellors as well as a network of specialized technical, legal, psycho-social and welfare services.

- **Expansion of technical solutions for lodging complaints:** A PANIC Button like the existing POCSO E-Box with NCPCR website should be created to trigger alarm and to route complaints on basis of priority to 1098 Helpline or the designated law enforcement officers.

- **Technically sound cyber nodals:** State police should appoint cyber nodals who have the technical competence for handling such complaints in a prompt and sensitive manner.

- **Proactive role of service providers:** Internet and mobile service providers should be engaged to create child online safety measures, products and simple, clear reporting channels. Mobile Associations and Ministry of Information Technology can create the platform for this.

- **Extensive training of trainers:** Fairly quickly a human resource corpus for providing online safety orientation and training should be created with the help of experts.

- **Production of information, education and communication materials:** In order to reinforce messages, various channels of information need to be employed. Social media, mass media, interpersonal communication, peer engagement, targeted campaigns, intergenerational communication and contracts - the opportunities are many and require creativity and strategy.

2. FRAMEWORK FOR CREATING PUBLIC AWARENESS MATERIALS ON BEING SAFE ONLINE

2.1 Objective

Children, caregivers and society are sufficiently informed about:

(i) Responsible use of information technology;

(ii) Risks and threats that children are exposed to online;

(iii) Prevention and reducing the risks;

(iv) Reporting cases of child online abuse and exploitation; and

(v) Seeking appropriate assistance, including social support, psycho-social counselling support, technical and legal assistance.

2.2 Guiding principles

(i) Positive and aspirational approach in educational initiatives;

(ii) Balancing children's rights to learn, access information and privacy with their right to protection through appropriate safety measures that do not restrict opportunities to ensure optimal online learning with minimal risks;

(iii) Active role of children based on their evolving capacities and resourcefulness in promoting online safety and digital citizenship; and

(iv) Age appropriate and relevant educational materials to serve three age groups, viz., 5-10 years, 11-14 years and 15-18 years.

2.3 Checklists for adequate and comprehensive information materials

Convention on the Rights of the Child	**Children's rights in the digital age**[1]	**Focus of materials for raising awareness on being safe online**
Protection 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)	Measures to prevent the creation and distribution of online child abuse imagery, sexual grooming, and online dimension of child trafficking.	Make children aware of the risks, the precautions they must take, and if need be where and how to report and where to seek help.
Protection from 'material injurious to the child's well-being' (Art. 17e), 'arbitrary or unlawful interference with his or her privacy, family, or correspondence, or unlawful attacks on his or her honour and reputation' (Art.16) and right of child to preserve his or her identity (Art. 8)	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)	Make children **aware of the various threats and risks**, the **preventive measures and safeguards** (Do's and don'ts), who/where to seek help from and report to.

[1] *Children's rights in the digital age. Adapted from Livingstone, S., and Bulger, M. (2014). A Global Research Agenda for Children's Rights in the Figital Age, Journal of Children and Media, 8:4, 317-335.*

Provision to support children's rights to recreation and leisure as appropriate to their age (Art. 31), an education that will support the development of their full potential (Art. 28) and prepare them 'for responsible life in a free society' {A. 29 (d)}	Measures to provide educational technology, online information and creative resources and promote digital skills equitably (factoring in differentials in languages, access or conditions of disability or disadvantage)	Child-friendly normative discussion on **digital citizenship** (including respect for the rights of other users), responsible use of information technologies and "good practices"
Recognizing 'the important function performed by the mass media' encourages **provision** of diverse material of social and cultural benefit to the child (including minorities) to promote children's well-being (Art. 17)	Measures to provide public and commercial educational, civic, science, cultural and heritage content online in an equitable way (as above)	Elements of **safe digital environment** for children as they seek diverse information materials through various online channels **Age-appropriate preventive online safety measures** (opposed to measures that restrict access) that could be shared with parents, educators and general public
Participation rights: 'In all actions concerning children… the best interests of the child shall be a primary consideration {A. 3(1)}, including the right of children to be consulted in all matters affecting them (Art. 12); see also child's freedom of expression {A. 13(1)} and freedom of association {A. 15(1)}	Measures to include all children in diverse societal processes, including consulting them on matters of education, research and ICT governance.	***Interactive models*** for seeking information, ideas and suggestions from children and young people [what is available or could be tested] **Development of materials for different groups of children** - gender sensitive content - varied levels of complexity for different age groups - access and usage differentials among urban, peri-urban and rural groups ***Group and individual counselling***

3. STANDARD CONTENT ON BEING SAFE ONLINE

3.1 Importance of Being Safe Online

Opportunities with threats

Digital technologies are here to stay in increasingly interconnected world, the mobile phones are any indication. They have become affordable and accessible for a major proportion of the Indian population. The fast expanding market is characterized by increasingly cheaper handsets and pricing incentives from the service providers. Urban areas have shown exceptional uptake and the rural areas are now showing exemplary expansion.

The digital technologies have an important role in national socio-economic development policies, and the Government of India's flagship Digital India provides a definite thrust in their promotion and expansion. These technologies are ubiquitous in various spheres of daily life of Indians, be it communication, banking, filing of taxes, sale and purchase of goods and services, and other financial transactions. The range of functions is expected to grow manifold and Indian languages are increasingly being employed in the apps to make them widely used.

However, many users use the gadgets to access services without adequate knowledge of the intricacies of digital technologies. They do not pay much attention to "the fine print" in the contract offered by the service providers. In the process, they remain unaware of the risks and threats they are vulnerable to. Mobile phones, tablets, and computers have similar as well as distinct features that the users need to be aware of. Some of the communication channels are "one to many" (e.g., emails, Facebook, Twitter) while some are "one-to-one" (e.g., WhatsApp).

Critical thinking, safe behavior and responsible participation by the users across board becomes imperative while the Government and its various arms and the IT sector are obliged to take measures to promote cyber safety and the responsible use of digital technologies. Unwary users are at risk in several ways even though various search engines (e.g., Google, Yahoo, Bing, Ask), social media platforms (e.g., Facebook, Twitter, LinkedIn, YouTube, Instagram, Pinterest) and messengers (e.g., WhatsApp, Skype) while providing diverse services are constantly seeking ways to offer safe experience for the users.

Against this backdrop, children and young people are and will be major consumers of digital technologies. As they stand to benefit, they are equally at risk. Controlling access and utilization is not feasible. Promoting resilience among them, i.e. the ability to deal with the risks and cope with the ill-effects with minimal damage, is likely to be a more effective and lasting strategy.

Why it is important to be a "digital citizen"?

The notion of digital citizenship is gaining currency as people are taking to cyberspace due to the promise of limitless opportunities. As the cyberspace is arguably not limited by the national boundaries and jurisdiction of domestic legislation, a new kind of social contract is called for. The starting point of digital citizenship are equal digital rights and supporting electronic access, which are critical in view of the Government of India's major boost to their use in advancing its policy agenda. Kerala has declared that internet is a basic human right and all citizens should have access to WiFi.

Digital citizenship is primarily about using technology appropriately and creating a culture where technology users are able to protect themselves. It has the following nine elements:

(i) **Digital access:** Help to provide and expand access to technology by recognizing that some that may have limited access and making efforts to ensure that no one is denied digital access.

(ii) **Digital commerce:** Make the users aware of the issues associated with legitimate and legal exchanges using digital technologies and how they can be effective consumers in a new digital economy. While the mainstream availability of Internet purchases of goods and services has improved, 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).

(iii) **Digital communication:** Communicate or exchange information with other people electronically, through emails, cell-phones and instant messaging, constantly and without delay. The technology users are expected to make appropriate decisions when faced with so many different digital communication options. But many of them do not.

(iv) **Digital literacy:** Educate people in a new way so that they are able to acquire high level of information literacy skills, including sophisticated searching and processing skills, which are required against the backdrop of rapid diffusion of ICT. Learners should be empowered to learn in a digital society, i.e. to learn anything, anytime, anywhere. As new technologies emerge, learners need to learn how to use that technology quickly and appropriately.

(v) **Digital etiquette:** Netiquette or etiquette on the internet involves respecting others' privacy and not doing anything online that will annoy or frustrate others. Email, online chat and newsgroups are the three areas where good netiquette is highly stressed. Do not spam other users with unwanted e-mails or flood them with messages. Observe how people communicate with each other after joining a newsgroup or online chat room before jumping in.

(vi) **Digital law:** Ethics is integral to digital citizenship. Abide by the laws of society. Users need to understand that stealing or causing damage to other people's work, identity, or property online is a crime. They need to be aware that certain rules apply to anyone who works or plays online. Hacking into others information, downloading illegal music, plagiarizing, creating destructive worms, viruses or creating Trojan Horses, sending spam, or stealing anyone's identify or property is unethical.

(vii) **Digital rights and responsibilities:** Use technology in a manner that respects the rights of others, including the right to privacy and free speech, that come with corresponding responsibilities. In a digital society, rights and responsibilities must work together for everyone to be productive. 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.

(viii) **Digital health and wellness:** Be aware of the inherent dangers of digital technologies, consequences of excessive use (e.g., eye safety and repetitive stress syndrome), sound ergonomic practices, and psycho-social issues that are becoming increasingly prevalent.

(ix) **Digital security (self-protection):** Protect information and equipment through responsible behavior ("good practices"), technological safeguards (e.g. access control, privacy settings, virus protection, backup of data, and surge control) and disposal of equipment.

3.2 How to Be Safe?

Being safe online

Internet is a great channel for connecting, accessing information and collaborating but the users, young and old, need to follow certain rules to remain safe in the online world. Every user of the Internet has a digital footprint, or a trail of data including the websites visited, the emails sent, and information submitted to online services. Consider the trail of data you are leaving behind. Remember that you are leaving your digital footprint before sending a scathing email, since the message might remain online forever. Be more discerning in what you publish on social media websites. While you can often delete content from social media sites, once digital data has been shared online, there is no guarantee you will ever be able to remove it from the Internet.[2]

Not everything online is trustworthy

- Recognize the importance of assessing the reliability of a website
- Evaluate the reliability and accuracy of online sources of information
- Other content (such as blogs, online adverts and search results)
- Contact (how others online may attempt to persuade us to follow a link, download a file or engage in other behavior).

Safe use of technology can be empowering

- Do not be a bully
- Do not remain a bystander if you encounter online abuse and exploitation

Online risks and threats can have far reaching effects

Online grooming: Strangers, or even people who are known, build an emotional connection with a child and young person 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.

The perpetrators are known to use several methods to entice the child:

- **Bribing:** This can range from offering money and gifts to the child. The gifts may even be in the form of even points, lives and in-game rewards in an online game.
- **Flattery:** They try to win the affection of the child by giving them constant attention and praise.
- **Sexualized games and intimacy building:** They test the child's vulnerability by introducing subtly sexual allusions in conversation or during play. If the child positively responds to his overtures, he will attempt to build further intimacy with the child.
- **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.
- **Threats and blackmail:** They employ forceful coercion to gain access to the child
- **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.[3]

[2]/techterms.com/definition/digital_footprint

[3] NSPCC

Online sexual exploitation: Internet has also emerged as a *means* to exploit children sexually, resulting in practices termed as "online", "ICT-facilitated" or "cyber-enabled" child sexual exploitation, which include all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. It includes any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted.

This notion can thus encompass (but is not limited to):

- Sexual exploitation carried out while the victim is online (such as enticing, manipulating and threatening a child into performing sexual acts in front of a webcam)
- identifying and/or grooming potential child victims online with a view to exploiting them sexually (whether the acts that follow are then carried out online or off-line
- distribution, dissemination, importing, exporting, offering, selling, possession of, or knowingly obtaining access to child sexual exploitation material online (even if the sexual abuse that is depicted in the material was carried out off-line)[4]

Identity theft: Fraudsters obtain personal information, including address, email address, previous addresses, mother's maiden name, place of birth, pin number, bank account details, Aadhaar number and passwords and use it in an unauthorized way for their personal gain. Such information is often required by companies or service providers as part of their verification process.

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.

The victims of financial fraud can also have a lot of issues come their way. If your details have been used in any form of monetary transaction, you could end up being saddled with debts. In most cases, if you can prove that the debts are not your responsibility, then you will not be liable for them. However, proving that you are not at fault can be difficult and time-consuming.

Legal implications of certain online action and content

Most users neither know nor understand the impact or the possible consequences of some of their online activities. Teaching them ethical and moral behavior in general, and an awareness of children's rights can create empathy for the victims of their communication and may address some problems such as cyberbullying, humiliating comments. However, they also need to be made aware about the legal implications of some of their online actions.

Children may also show extra bravado because they have the illusion that their actions online are anonymous and that "nobody will ever know".

[4] http://luxembourgguidelines.org/english-version/

Please note that the following are legal offences: *Details of offences and the relevant sections of different legislation have been provided here for the information and knowledge of the programme planners. These will need to be incorporated according to the evolving capacities of children and young persons and their age appropriate information requirements. These can also be suitably adapted for the different adult stakeholders.*

Voyeurism and violation of privacy

Section 354C, the Indian Penal Code (IPC) 1860: Viewing and/or capturing the image of a girl or woman going about her private acts, where she thinks that no one is watching her is a crime. This includes a woman, using a toilet, or who is undressed or in her underwear, or engaged in a sexual act.

It may not be a crime if a girl or woman agrees to taking of her private photos, it can certainly be risky. However, if she expects them to remain with only certain people, then sharing them is a crime. She must expressly consent to both, watching/taking pictures as well as sharing them, for it to not be an offense. The offender in such cases of voyeurism can be punished with three to seven years of imprisonment and a fine. While this section of the IPC can only be used by girls and women, the Information Technology Act, 2000 is gender neutral.

Video voyeurism

Section 66E, IT Act, 2000: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding Rupees two lakh or with both**.**

Explanation: For the purposes of this section,

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons:

(b) "capture" with respect to an image, means to videotape, photograph, film or record by any means

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast

(d) publishes" means reproduction in the printed or electronic form and making it available to public

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that

  (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

  (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Stalking

Section 354D, IPC, 1860: Continuously following a woman or contacting her, either online or in person, and where she has clearly shown that she does not want the attention is a criminal offence. It is punished by three years for a first offense, and five years for repeat offenses. The only exception is when a person is stalking a woman as a legal duty.

Sending obscene material without the consent of the recipient

Section 354A, IPC, 1860 (sexual harassment): it includes the act of showing pornography against the will of a woman.

Section 67, IT Act, 2000: It punishes sharing obscene material in electronic form. The punishment can be jail for five years and a fine of Rs 10 lakhs.

Section 67A, IT Act, 2000: It punishes sharing material containing sexually explicit act in electronic form with jail for seven years and a fine of Rs 10 lakhs. The provisions of the Information Technology Act are not gender specific and apply to everyone.

Use of child for pornographic purposes

Section 13, Protection of Children from Sexual Offences (POCSO) Act, 2012: 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:

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.

Section 14, POCSO Act, 2012: (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 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.

Section 67, IT Act, 2000 (Publishing or transmitting obscene material in electronic form): Whoever,

- publishes or transmits or causes to be published 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 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 Rs 10 lakh.

Section 67A, Information Technology Amendment Act (ITAA), 2008 (Punishment for publishing or transmitting of material containing sexually explicit acts):
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 Rs 10 lakhs 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 Rs 10 lakhs.

Section 67B, IT Act, 2000 (Transmitting material depicting children, including nude or sexually explicit pictures of self, if a child):
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 a fine which may extend to Rupees ten lakh 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 Rupees ten lakh:

Sexual harassment

Section 11, POCSO Act, 2012: A person is said to commit sexual harassment to 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 shows any object to a child in any form or media for pornographic purposes; or
III. shows any object to a child in any form or media for pornographic purposes; or
IV. any other means; or repeatedly or constantly follows or watches or contacts a child either directly or through electronic, digital 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 12, POCSO Act, 2012: Whoever, commits sexual harassment upon a child shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable for fine.

Section 354A, IPC, 1860: It provides for punishment of jail between one and three years for making a demand for sexual favors and making sexually colored remarks towards a woman

Section 509, IPC, 1860: It deals with word, gesture or act which intends to insult the 'modesty' of a woman.

Section 509 can also be applied for intrusion of privacy intending to insult the modesty of a woman if a person obtains a woman's contact details and tries to contact constantly against her will. The IPC is not very clear about the meaning of "modesty of a woman" but the Courts usually make the determination based on the circumstances surrounding the incident. The Supreme Court referred to 'modesty' as "feminine decency" and a virtue that women possess due to their sex. For Section 509 to apply, the offender should have uttered any word, made a gesture or sound, or exhibited any object, or intruded on the privacy of a woman, with the intention that this should be seen and heard by the woman. The punishment can be a term of simple imprisonment up to three years.

In addition to the above-mentioned provisions in the IPC that that apply only to females, there are other laws which apply generally. Section 294 of the IPC punishes any obscene words uttered in a public place. Section 295A of the IPC punishes words, either written or spoken, which insult someone's religions or religious beliefs. Section 3(1)(x) of the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act deals with caste-based abuse. Section 503 of the IPC deals with threats to injure any person, their reputation, or their property and Section 506 of the IPC provides for a jail term of seven years and a fine as punishment for criminal intimidation.

Revenge porn

Victimizing by way of revenge porn has become a common phenomenon in India now. This is often also 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."[5]

While revenge porn essentially creates sexual violence against girls and women, it necessarily involves voyeurism, hacking, stalking, and violation of privacy. There is no specific law for revenge porn but the offences can be regulated by applying Section 354C, IPC (Voyeurism), Section 66E, IT Act (violation of privacy) and Section 509, IPC (harming the modesty of women). Revenge porn should also be seen in the perspective of indecent representation of women.[6]

[5] Halder and Jaishankar, 2013.

[6] Halder and Jaishankar, 2013.

Hacking of account or creating a fake account in someone else's name: Section 66C, IT Act, 2000 which deals with identity theft, provides for jail for three years a fine of Rupees one lakh if it is shown that someone stole or dishonestly used another person's password, digital signature, or any other unique identifying feature. Section 66D provides similar punishment for cheating by personation by using a computer source, i.e., if someone creates a fake social media account in someone else's name and cheats anyone through it.'

Identity theft, Section 66C IT Act, 2000: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term that extends up to three years and shall also be liable to fine which may extend to Rupees one lakh.

Section 66D, IT Act (Impersonation), 2000: Whoever, by means of any communication device or computer resource cheats by personation (*assumes the identity of someone else with the intention of fooling or deceiving the person*) shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to Rupees one lakh.

Section 66B, IT Act, 2000 (Stolen Computer): Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe that the same to be a stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to Rupees one lakh or with both.

Video and audio piracy: Watching movies on copied DVDs or downloaded from Torrent sites may not currently be a crime in India, it certainly is in many countries as such acts constitute infringement of copyright.

In the wake of messages that several internet service providers posted on their websites, the Bombay High Court ruled that "the offense is not in viewing, but in making a prejudicial distribution, a public exhibition or letting for sale or hire without appropriate permission copyright-protected material." The messages by the ISPs, displayed when users try to open blocked websites, said, "Viewing, downloading, exhibiting or duplicating an illicit copy of the contents is punishable as an offence under different sections of the Copyright Act, 1957."

Downloading movies, music and copyright content from the internet is against the Indian copyright law, as are uploading copyright content to the web. By the way, saving images off the web, uploading them elsewhere like Reddit, making memes out of them, using them in your projects, etc are illegal too. That image does not belong to you; its copyright belongs to someone else, so you can't profit from it without their permission.

How can the risks be reduced?

Securing oneself online through responsible use and self-regulation: Read the terms and conditions for the use of social media platforms. Do note that you are giving a lot of your personal data when you sign up. Small print often contains hidden clauses waiving privacy rights and allowing the posted content to be sold on.

Sample Quiz

1. What is the minimum age for opening an account on the following?
   (i) Facebook
   (ii) Instagram
   (iii) Twitter
   (iv) Snapchat

Answer: (i-iv) 13 years. Just because children seem tech-savvy at increasingly younger ages, doesn't necessarily mean that their brains are developing at the same rate as their digital acumen.

2. Why is it important for the accounts to private?
3. Whose photographs can one post online?

Cyber bullying: Children who are bullied online often feel hurt and rejected by their peers, which can lead to low self-esteem and depression.

- Do not respond or retaliate. Be civil.
- Save the evidence. Take "Screen Shots" using the Snipping Tool in Windows. The mobiles also have a feature to take screen shots.
- Talk to a trusted adult or report to authorities
- Block people who bully or make you uncomfortable or who you do not know. All social media platforms have a feature that allows you to block. Do you know where it is? So example in Facebook click on the report option you have an option to BLOCK.

How to protect against phishing attacks?

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

Use unique passwords: Many people use the same password for multiple websites. This is a terrible mistake. If your credentials are stolen on one site and you use the same username and/or password on others, it's simple for the cybercriminal to get into each account. **Go the given link to find out how to create hack-proof passwords.**

Set up a two-factor authentication: Two-factor authentication, also known as two-step verification, means that to log in to your account, you need two ways to prove you are who you say you are. It's like the DMV or bank asking for two forms of ID. **Go the the given link to learn how to set up two-factor authentication.**

Have strong security software: Protecting your gadgets with strong security software is a good defense against digital threats.

How to protect against pharming?

If a certain website appears to be significantly different than what you expected, you may be the victim of pharming.[7]

- Restart your computer to reset your DNS entries, run an antivirus program, then try connecting to the website again.
- If the website still looks strange, contact your ISP and let them know their DNS server may have been pharmed.

Taking appropriate action to reduce online risks and threats

Prevent malicious or undesirable contacts through use of

- Preferences
- Privacy tools
- Pop-up blocker

Technology related measures

Good practices to protect accounts and enhance online security:

- Select unique and strong passwords that are difficult to guess
- Do not share passwords
- Learn to block
- Control access
- Install firewall
- Use updated anti-virus software
- Use filtering software
- Use privacy settings and sharing controls

Precautions before disposing equipment

Measures to take before giving away or selling off old mobiles and computers:

- If you wish to transfer information from the old device to your new phone, simply do so before clearing the old one.
- Remove your information from the device you wish to dispose-off as phones tend to allow access to sensitive, personal information by performing a factory reset.
- Removing the SIM and SD cards as these cards also store personal information that a factory reset will not erase. You may also wish to keep your SIM card so that you can retain your old phone number by having the card transferred into your new device.

Once your phone has been rid of personal information, you may now safely dispose of it.

Measures to take before trashing electronic waste

If you must throw away your phone, it is important to do so in a safe, environmentally conscious way. If your phone is not in good enough condition to be given away, do not simply throw it in the

[7] https://techterms.com/definition/pharming

trash. Phones contain toxic chemicals that, when a phone is placed in a landfill, may ultimately leach into groundwater and poison the water in surrounding areas. Discarding of phones with the garbage also poses a danger to workers who crush trash.

Look out for programmes for recycling or safe and green disposal of phones or other electronics. These are few but offered increasingly by some mobile phone vendors or technology-centered companies. If such a receptacle cannot be located, contact local health and sanitation agencies and inquire about their preferred means of discarding electronics.

Online Risks and Threats to children *(read in order from younger to older age groups*)

- Exposure to Inappropriate or obscene material (also known as child sexual abuse materials or CSAM)
- Misuse of private and personal information
- Harmful and illegal content
- Sexual Harassment
- Invasion of Privacy
- Excessive gaming
- Hacking Digital Identity
- Digital Reputation/ Cyber defamation
- Cyber Stalking
- Cyber Bullying
- Cyber Predation
- Cyber Pornography
- Grooming
- Trolling
- Happy Slapping
- Rumor Mongering
- Phishing
- Scams and Schemes
- Intellectual Property Crimes
- Copyright Infringement and Plagiarism
- Cyber Terrorism
- Leaving Digital Footprints or trail for harmful use

Cyberbullying is when someone uses technology (such as the internet or a mobile phone) to bully others. Being a victim of cyberbullying can be very distressing for a young person as most of the time they don't know who is bullying them. Cyberbullying includes things such as sending nasty text messages or emails, or setting up a hate group on a social networking site. The bullying may also happen 24/7 and the victim is often targeted even when they are in the comfort of their own home. Images and text messages can be circulated very quickly and widely on the internet which makes it very hard to combat cyberbullying.

Audience-specific Information

Parents and Guardians

The internet is always changing, and being able to keep up to date with your children's use of technology can be a challenge, especially if you feel that your children may have better technical skills than you do. However, children and young people still need support and guidance when it comes to managing their lives online and using the internet positively and safely.

Watch your children and ask yourself, are they:

- Eating and sleeping enough?
- Physically healthy?
- Connecting socially with friends and family – through technology or otherwise?
- Engaged in school?
- Enjoying and pursuing hobbies and interests – through technology or beyond?

If the answer to these questions is more or less "yes," then you need not worry. But if the answers are "no" then you need to negotiate 'screen time' with your children.

- Be aware of the benefits and risks that the internet offers
- Communicate regularly with children about what they do online, encourage them to talk about problems they may find
- Install firewall, anti-virus software, filtering software or other technical measures
- Use privacy settings and sharing controls
- Support them to deal with social/ peer pressure

Prevention of misuse

Intergenerational dialogues:[8] Have a conversation. A simple and effective way to get involved with your children and their lives online is through discussion. By maintaining an open dialogue with their child and encouraging them to talk to you about their internet use parents can help children access the amazing resources the internet has to offer whilst keeping them safe online.

- Ask your children to tell you about the sites they like to visit and what they enjoy doing online.
- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is OK and not OK to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
- Encourage them to help. Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you use the internet as a family. What could you do to get more out of the internet together and further enjoy your lives online?

[8] http://www.childnet.com/parents-and-carers/hot-topics/parental-controls

Check age restrictions: Many online services have age limits restricting who can use their services. Always check a website's terms of use before allowing your child to sign up for an account, and be clear with your kids if you have family rules about which sites and services they can use.

The following list is not exhaustive but provides some common symptoms that deserve attention as they may indicate grooming:

- The child spends inordinate time on the internet
- He or she is extremely secretive about internet activity
- He or she speaks of friends you do not know
- He or she has new possessions (e.g., toys, clothes, gadgets that he or she cannot explain how they got hold of).

Speak to your child about the issue and make sure they understand what 'grooming' means. Communicate that 'things are not what they seem to be on the internet' but do not indulge in blaming the child. Instead, consider seeking professional counselling.[9]

Parental Controls[10]

Designed to help protect children from inappropriate content they may come across online, such as pornography, parental controls can be used to limit access to only age-appropriate content, to set usage times and to monitor activity. They are located at four sites and their combination can protect children.

(i) ***Internet provider:*** You can set up filters to help block access to inappropriate content on any device connected with your home WiFi;

(ii) ***Mobile operator:*** Filters are often automatically set up on mobile contracts but you can double-check with your provider;

(iii) ***Devices:*** Many devices have parental control settings, e.g., to help restrict spending in apps or to disable location functions; and

(iv) ***Online services:*** some sites like iPlayer and YouTube have parental control settings to help restrict access to inappropriate content

However, no parental controls or filtering options are 100 per cent effective. When children are tech-savvy, they may disable these parental controls. Be aware also that once parental controls by your internet provider are set up on your WiFi, if your child access 3G or 4G at home, the parental controls can be bypassed. Similarly, if your child goes to their friend's house where there are no parental controls in place, they will be able to access whatever they want. For these reasons, it's important to educate your child about the potential risks online, and establish rules concerning the sites that are suitable, or inappropriate, to visit.

Attending to risks while promoting online opportunities is the rule to follow - Paying too much attention to reducing risk may have the adverse effect of limiting children's opportunities. However, promoting online opportunities without highlighting the potential risks may also result in online harm. Promoting online opportunities and making children aware of their own online safety needs to be balanced.

[9] NSPCC

[10] http://www.childnet.com/parents-and-carers/hot-topics/parental-controls

Remember not to pull the plug! While it is good to keep an eye on your child's online activities, be certain that you cannot track everything your child does and it is never appropriate to stop total access based on anything wrong they may have been done.

It is advisable to have an open channel of communication with your child and help them to develop the skills and knowhow to be a safe online player, whatever technology they use, and have resilience to bounce back in the event that anything goes wrong. They cannot survive and thrive without these skills.

Teachers and Schools

Proposed actions for schools

Schools and teachers

- Develop "whole school" policies regarding positive uses of technology as well as protocols to deal with instances of online bullying and harassment
- Ensure provision of ICT and digital skills development for teachers and staff, supported by awareness raising about risks and online safety of their students and the school's rules and policies.
- Engage with students, parents and guardians to send a common message on online safety.
- Activities that use new technologies can make a really valuable contribution to the wider school curriculum and to children's learning. It is essential for educators to recognize the benefits of technology and understand the many different ways that children and young people are using internet enabled devices, especially in the home and within social environments
- At times it can be hard to keep up with changes in the use of technology and so the Hot topics section contains information regarding a variety of internet safety issues including gaming, social networking, cyberbullying, grooming, sexting, downloading and file sharing.
- Teach students to develop a critical eye in order to learn to assess and select trustworthy information, and keep track of their digital footprints

What can I do to help as an educational professional?

1. **Understand the tools:** Be aware of the reporting mechanisms on different sites and services so you can support your pupils in making a report.
2. **Discuss cyberbullying:** Be proactive in discussing cyberbullying with your pupils; how it occurs, why it occurs, and the consequences of such behavior.
3. **Know who to report to:** Ensure that you are aware of who to go to in your school or organization if you have concerns about cyberbullying incidents. This may be the IT teacher or school counsellor, a member of the senior leadership team, or a staff designated for the purpose.

What advice is there for schools?

- Incorporate child online safety in the child protection policies of the school and establish protocols for reporting offences and supporting children who have been victimized or are at risk
- Organize periodic orientation on online safety for children and encourage them to share their concerns, and for teachers and encourage them to keep the conversation on online safety with children ongoing
- Appoint counsellors/ focal points who can provide immediate assistance to children in need
- Organize periodic sessions on parental education
- Make available information, education and communication materials that children can access easily
- Engage children in regular activities for promoting child online safety, e.g. online safety champions, mentored by teachers and experts, who can reach out messages to their peers

Some activities for children

Objective: To recognize the importance of assessing the reliability of a website and to evaluate the reliability and accuracy of online sources of information.

ACTIVITY 1 ***(10 mins)***

Copy the following statements onto the board and ask the students to mark them as True or False in their notebooks. [If the students have access to devices connected to the Internet, we recommend that the activity be completed using Google Forms.[11]

True or False?[12]

- If I can find it online, it must be true. (F)
- I should always check the sources and authors of a website. (T)
- There's a contact email address on the website, so it must be a legitimate site. (F)
- There's a government logo at the top of the page. I can trust this site. (F)
- I should always compare information that I find online with at least two alternative sources. (T)
- There are lots of graphics and charts on the site. All that information means it must be reliable. (F)
- It's clear who wrote the content because the site has contact information, seems reliable and is error free. I can therefore use this information in my schoolwork. (F)
- The website looks official. The information on it must be reliable. (F)

ACTIVITY 2 ***(10 mins)***

1. What makes a website trustworthy? Ask your students to list the factors that they believe make a site trustworthy, and then share that with the rest of the class.
2. Discuss all the factors mentioned with the group, emphasizing the following points:

- Anybody can write something on the Internet.
- Although there are lots of true and interesting things on the Internet, we can't always be sure that everything we find is accurate.
- Not everyone is an expert on the things they write about.
- Given that we do not always know who wrote the information, or if they have the necessary expertise to write about a subject, we must be careful and verify any information before accepting it as true.

3. Ask the students to make a note of the criteria that should be used to assess the reliability of a website.

i) Who: Aptitude of the author

- Is the author identified on the page?
- Is there any information on the author's education or occupation?
- Are references quoted from reliable sources?
- Are there any links or referenced sites?
- Is it opinion, or information derived from a research project?

(ii) What: Domain and objectives of the site

- Is the site maintained by the Government, educational institution or commercial organization?
- What country is the website from? (verify the domain: .us for the USA, .uk for the UK, .au for Australia)
- What's the purpose of the site (sell, inform, etc.)?
- Who is the website aimed at?

[11] https://docs.google.co.uk/forms

[12] Google.

(iii) When: Updates

- If updated information is required, it's worth finding out when the content was published. Is the information current? Is it still in force?
- Is the website updated regularly? Can you find any out-of-date links?

(iv) Other criteria:

- Are there any spelling mistakes?
- Is the writing clear?

ACTIVITY 3 ***(10 mins)***[13]

Technical requirements: A computer or tablet for each group of students.

Explain to the students that they are going to assess online sources of information by trying to answer the question: Is there life on other planets? Organize the students into groups and ask them to complete the information in the table for each website:

Website 1: http://www.livescience.com/47246-alien-life-in-solar-system-candidates.html
Website 2: http://spaceplace.nasa.gov/review/dr-marc-solar-system/life-on-mars.html
Website 3: http://www.latest-ufo-sightings.net/

Sexting [verb] = sending a sexually explicit message

The term 'sexting' describes the use of technology to share personal sexual content. It's a word-mix of sex and texting. Young people tend not to use this term but may use other nicknames such as 'nudes', 'nude selfies' or imply these through the context of the message.

What else do I need to know about sexting?

The content can vary, from text messages to images of partial nudity to sexual images or video. This content is usually created to be sent to a partner but can be between groups or even for a dare. Such images can be created using a range of mobile devices, technologies and online spaces. Photos and videos are often created via webcam or smartphone cameras, and are shared on social networking sites such as Snapchat, Instagram, Facebook, Twitter and video-sharing sites such as YouTube.

This behavior is not exclusive to students in a secondary school as the motive behind it may not always be a sexual one. For younger children, it may be sent as a dare or as part of them exploring their bodies and relationships with others.

What advice can I give to my pupils?[14]

(i) **Resist peer pressure:** The creation of sexting content is quite often due to pressure from a partner or group. Discussing peer pressure with students is a positive way to encourage them to take responsibility for their own actions and resist pressure from others to engage in activities they are uncomfortable with, or know to be against the law.

(ii) **Know the law:** Although pupils may be treated as victims in instances of sexting, it is important to educate them about how such behavior breaks the law, and the potential consequences.

[13] Google
[14] http://www.childnet.com/teachers-and-professionals/for-working-with-young-people/hot-topics/sexting

(iii) **Understand the consequences:** increasing your pupils' awareness about what can happen after sexting content has left their control is very important in helping them to understand the effects that may have on their reputation and psychological well-being; both short term and long term.

(iv) **Losing your inhibitions could lead to loss of control:** the distribution of sexting content is often deliberate but can also happen in a less planned way, for example through spontaneity or peer pressure, or if a young person is under the influence of alcohol or drugs and their judgement is impaired. Remind your pupils that they have control over the images they create and share, but once they have shared that content, it is out of their control.

(v) **It's never too late to tell someone:** encourage pupils to speak to someone they trust if they are involved in a sexting incident. Although it may feel like the end of the world to a young person, there is always a way back. The quicker they speak to someone, the better the chance of managing the spread of the content.

(vi) **Report it:** If an image of this nature has ended up being shared more openly on websites or social media then it is important to use the reporting tools available. A young person can contact the social media platform immediately to begin with if they are concerned that their image has ended up online and they need support in removing it.

Where does the law stand?

If a person under the age of 18 engages in sexting by creating an explicit photo or video of themselves then they have potentially created an indecent image of a child. By sending this content onto another person, they have distributed an indecent image of a child. By receiving content of this kind from another young person, they are then in possession of an indecent image of a child.

What are the other risks?

Reputation damage: with young people connecting via a wide range of technologies and social media sites, sexting content can be distributed to other users very quickly. This prevents the young person from controlling where the content is posted. This can result in damage to a young person's reputation in their school or local community, and in online communities. As content posted online can potentially exist forever in the public domain, this can have longer term effects on a young person's reputation and aspirations.

Emotional and psychological damage: the distribution of sexting content to others can cause distress and upset to the young person involved, especially if the content is distributed by someone they entrusted it to. The effects of others seeing this content can lead to negative comments and bullying, and may result in a young person losing confidence or self-esteem, and in extreme cases could lead to depression and other physical harm.

What advice can I give to young people?

Mentor students, promote positive, safe, and effective use of the internet by children in all educational contexts.

(i) Be aware of the benefits and risks that the internet offers;

(ii) Prepare a list of "safe" websites to encourage online learning in a safe environment;

(iii) Integrate online safety awareness and digital skills across the curriculum;

(iv) Ensure that all children benefit from digital technologies;

(v) Use privacy settings and sharing controls; and

(vi) Support them to deal with Social/ Peer pressure

The internet is an amazing resource and can be used in a number of positive ways. However, content posted online can be easily misunderstood by others and taken out of context. It is important for young people to recognize the importance of '***thinking before you post***' and the need to ***respect their friends' and peers' thoughts and feelings online***. What is considered morally right and wrong offline must also be thought of in the same way online, and treating others with respect on the internet is a good way to ensure that online situations are less likely to escalate into cyberbullying situations.

Don't reply: most of the time the bully is looking for a reaction when they are teasing or calling someone nasty names. Remind young people not to reply, if they do they're giving the bully exactly what they want.

Save the evidence: Encourage young people to save the evidence of any emails or text messages they receive (e.g., screenshots and email trail). This would enable them to report cyberbullying.

Tell someone: encourage young people to tell a trusted adult if they are being cyberbullied, and to tell them as soon as they can in order to minimize their own upset or worry.

Children and Young People

Exercise caution

- Agree with family and/or teachers to access only websites jointly identified as safe
- Recognize ways that people online may seek to persuade you
- Make decisions about what might be trusted using different criteria; evaluate the trustworthiness of online content.
- Create usernames that never reveal true identity
- Create strong, unique and easy to remember passwords for online account.Keep your information and passwords private
- Promise to inform and discuss with family members any annoying or uncomfortable occurrence or activity such as cyber stalking, bullying and strange behavior on computer and applications, mobile.

Golden rules to follow when online[15]

- Do not give out personal information (e.g., address, phone number or email).
- Do not react or respond when faced with bullying or offensive content but block/report such incidents and keep record
- Do not share inappropriate pictures with anyone, especially pictures nude or semi-nude pictures,or pictures that reveal school,location etc.
- Do not open emails or attachments from people you do not know.
- Do not become online 'friends' with people you don't know.

[15] Do's and Don't: http://www.infosecawareness.in; http://www.childnet.com/young-people/primary/need-help

- Remember not everyone online is who they say they are.
- Remember not to give out information on locations you go to frequently with your friends.
- Never arrange to meet someone in person whom you've met online.
- If anything you see or read online worries you, makes you feel unsafe or uncomfortable, turn off your computer and tell someone/inform your parents or a trusted adult about it immediately.

Older children

- ***Protect your online reputation:*** use the services provided to manage your digital footprints and 'think before you post.' Content posted online can last forever and could be shared publicly by anyone.
- ***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's never too late to tell someone.
- ***Don't give in to pressure:*** if you lose your inhibitions you've lost control; once you've pressed send you can't take it back.
- ***Respect 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.

How to create strong and unique passwords[16]

- Use at least 8 characters or more to create a password.
- The more number of characters one uses, the more secure is the password.
- Use various combinations of characters while creating a password. For example, create a password consisting of a combination of lowercase, uppercase, numbers and special characters etc.
- Avoid using the words from dictionary. They can be cracked easily.
- Create a password such that it can be remembered. This avoids the need to write passwords somewhere, which is not advisable.
- A password must be difficult to guess.
- Change the password periodically or when you suspect someone knows the password.
- Do not use a password that was used earlier.
- Be careful while entering a password when someone is sitting beside you.
- Do not use the name of things located around you as passwords for your account.

Online reputation[17]

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. It is made up of the content you create, post and share; as well as the content that others post, and share, with you and about you. It can be positive or negative and affects how people see you now or in the future. Use the simple checklist to help manage and maintain your online reputation.

[16] http://www.infosecawareness.in
[17] http://www.childnet.com/young-people/secondary/hot-topics/online-reputation

- **Search yourself online:** do you know what is online about you? Do a simple web search of your name and see what you can find. If you find something you aren't 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.
- **Make a positive footprint:** we hear a lot about the negative footprints left behind online. 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.

3.3 Reporting

Sharing problems to seek solutions

There are lots of people who can help! Your friends and adults whom you trust.

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. 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**.

Inappropriate contact: If you have been in touch with someone online, and conversations with that person are making you feel uncomfortable tell an adult you trust. You can also report these to **Childline at 1098.**

Seeking advice and mediation from people you trust

Parental Support: It is easy to speak with and seek help from parents if some kind of "family agreement" has been arrived at through dialogue within the family. Parents do need to keep themselves informed and ensure openness and sensitivity in their communication with children. Information is available online for parents to educate themselves. For instance, Cybermom is a mechanism that is in place in many countries including India, which provides useful and easily comprehensible information.[18]

Peer Group Support: It is also easy for children and young people to communicate with peers, especially those who know more about the problems or have had similar experiences, without the fear of being judged. Peer advisors should be trained, coached and mentored for roles and responsibilities that require a certain level of knowledge and sensitivity. There could be lessons from peer education programmes that are being implemented by some of the ICT companies and organizations.

Contacting the social media platform

Process and mechanism for blocking offensive content

The first step can be to try and approach the social network to get the pictures taken down.

How to remove photos?

Select the provider where the picture/video is being displayed.

1. **Include your age:** It is important to tell them if you are a child/youth. Include your age at the time the picture/video was taken as well as your current age.
2. **Say that you are the person in the picture/video:** If you are recognizable in the picture/video, include this as well – this may give your report a higher priority.
3. **Say that you did not post the picture/video, did not agree to it being posted and want it removed:** They need to know that you object to the continued posting of the picture/video.

[18] https://cybermumindia.wordpress.com

4. **Let them know if you sent the picture/video to someone else:** Include those names as most providers set out rules for the type of content that can be posted and those who break the rules may be prevented from posting content in the future.

Mobile	Desktop/laptop
Facebook	
● Tap () at the top right corner of the page. ● Scroll to the bottom of the list and tap "Report a Problem". ● Select a product (i.e. "Profile", "Photos", or "Pages") from the list provided in the drop-down menu. ● In the "What went wrong?" text box, include the information outlined in the four points above. ● You have the option to attach a screenshot of the reported content. Note: If the picture/video being reported contains individuals under the age of 18 whose sexual organs are visible and/or who are engaged in sexual activity, we suggest that you do NOT screen capture this content. ● Tap "Submit".	● Click on the picture you would like to report. Scroll to the bottom of the picture and click "Options". ● Select "Report photo" or "I don't like this photo". ● If applicable, click "I think it shouldn't be on Facebook". ● Click "Continue". ● Select the most appropriate category from the options provided (i.e. "This is nudity or pornography") and click "Continue". ● Click "Submit to Facebook for Review". For complaints about content (pictures, videos) posted on an individual's Facebook profile: ● Click the '…' on the bottom right corner of the person's profile picture which also includes a drop-down menu (next to the "Message" button). ● Select "Report". ● Continue by selecting "Report this profile". Click "Continue". ● Select the most appropriate response (i.e. "They're sharing inappropriate or offensive posts"). Click "Continue". ● Select the most appropriate category (i.e. "Nudity and pornography"). Click "Continue". ● Select whether you would like to contact the user or unfriend the individual. Click the box "Submit to Facebook for Review".
Twitter	
1. Access https://support.twitter.com/forms/abusiveuser. 2. Select the most appropriate option regarding how you are involved (i.e. "Directed at me"). 3. Select the most appropriate type of complaint (e.g. "Harassment" or "Specific violent threats involving physical safety or well-being"). 4. Complete the form, including providing a link to the content, the individual's username, Twitter username, and email address in the appropriate fields.	For complaints regarding pictures/videos posted on Twitter: ● Go to https://support.twitter.com/forms/abusiveuser. ● Select the most appropriate option regarding how you are involved (i.e. "Directed at me"). ● Select the most appropriate type of complaint (e.g. "Harassment" or "Specific violent threats involving physical safety or well-being").

5. Fill out the questionnaire based on information about the reported content. 6. In the field marked "Further description of problem", provide the information outlined in the four points above. 7. Tap "Submit".	● Complete the form, including entering a link to the content, the individual's username, Twitter username, and email address in the appropriate fields. ● Fill out the questionnaire based on information about the reported content. ● In the field marked "Further description of problem", provide the information outlined in the four points above. ● Click "Submit". For complaints regarding child pornography content: ● Access https://support.twitter.com/forms/cse. ● Select the most appropriate option regarding how you are involved (i.e. "Directed at me"). ● Complete the form, including providing a link to the content, the individual's username, and YOUR email address. ● In the field marked "Anything else?", provide the information outlined in the four points above. ● Click "Submit". You can also lodge a complaint regarding child pornography content by sending an email to cp@twitter.com and include the link to the profile and links to any relevant tweets displaying the content. Also include the information outlined in the four points above.
Instagram	
To make a complaint about a picture on Instagram: ● Access http://help.instagram.com/contact/383679321740945. ● Select the most appropriate category (i.e. "Photo or video"). ● Next, select the most appropriate type of complaint (i.e. "Nudity or pornography" or "Self-harm or suicide"). ● Select whether you have an Instagram account or not. Of note: If choosing "No", you will be required to fill in additional details. ● Complete the remainder of the form. In the text box, include the information outlined in the four points above. ● Tap "Send".	To make a complaint about a picture on Instagram: ● Go to http://help.instagram.com/contact/383679321740945. ● Choose the most appropriate category (i.e. "Photo or video"). ● Select the most appropriate type of complaint (i.e. "Nudity or pornography" or "Self-harm or suicide"). ● Select whether you have an Instagram account or not. Of note: If choosing "No", you will be required to fill in additional details. ● Complete the remainder of the form. In the text box, include the information outlined in the four points above. ● Click "Send".

<table>
<tr>
<td>To make a complaint regarding a user threatening to post sexual images on Instagram:
Sign in to Facebook using your Facebook username and password.
Access https://www.facebook.com/help/instagram/contact/584460464982589#_=_.
Complete the form to report photos, videos, comments, or profiles on Instagram that are bullying or harassing others by selecting the most appropriate options.
Depending on your selections you may have the option to attach a screenshot of the reported content. Of note: If the picture/video being reported contains individuals under the age of 18 whose sexual organs are visible and/or who are engaged in sexual activity, we suggest that you do NOT screen capture this content.
Tap “Send”.</td>
<td>To make a complaint regarding a user threatening to post sexual images on Instagram:
Sign in to Facebook using your Facebook username and password.
Access https://www.facebook.com/help/instagram/contact/584460464982589#_=_.
Complete the form to report photos, videos, comments, or profiles on Instagram that are bullying or harassing others by selecting the most appropriate options.
Depending on your selections you may have the option to attach a screenshot of the reported content. Of note: If the picture/video being reported contains individuals under the age of 18 whose sexual organs are visible and/or who are engaged in sexual activity, we suggest that you do NOT screen capture this content.
Click “Send”.</td>
</tr>
<tr><td colspan="2">YouTube</td></tr>
<tr>
<td>Sign in to the service using your username and password.
Flag the video as inappropriate by tapping the flag icon located below the video, to the right.
Tap “OK”.
Select the reason you are flagging the video (i.e. “Sexual Content”).
Tap “Flag This Video”.</td>
<td>Sign in using your YouTube username and password.
Flag the video as inappropriate by clicking the link “••• More” located below the video and click “Report”.
Select the most appropriate issue from the options provided (i.e. “Sexual content”).
Select the most appropriate category from the list provided (i.e. “Content involving minors”).
Enter the specific time for where the content you are reporting is located within the video (e.g. if the content you’re concerned about appears at 15 minutes and 30 seconds, enter 15:30). If you are concerned about the entire video, enter the length of the video.
In the text box, provide the information outlined in the four points above.
Click “Submit”.</td>
</tr>
<tr><td colspan="2">Google</td></tr>
<tr><td colspan="2">Pictures that appear on Google image results are actually hosted by a different service (i.e. not Google). In order to remove pictures that appear in Google image results:

1. Submit a report to the website where the picture is being displayed: To determine where the picture is displayed, access the picture in the Google search results and view the full image. This will provide the website address for the picture. Information about the website where the picture is displayed can be found within the website address for the picture.</td></tr>
</table>

If the website address for the picture is http://www.websitedomain.ca/imageinformation.jpeg, the site where the picture is displayed would be http://www.websitedomain.ca. Access this website and look for information about how to contact the provider to request the removal of your picture/video.

When contacting the provider:

a. Include your age: It is important to tell them if you are a child/youth. Include your age at the time the picture/video was taken as well as your current age.

b. Say that you are the person in the picture/video: If you are recognizable in the picture/video, include this as well – this may give your report a higher priority.

c. Say that you did not post the picture/video, did not agree to it being posted and want it removed: They need to know that you object to the continued posting of the picture/video.

d. Let them know if you sent the picture/video to someone else: Include those names as most providers set out rules for the type of content that can be posted and those who break the rules may be prevented from posting content in the future.

2. **Dealing with cached website content:** Once a picture/video has been removed from a website, the content may continue to appear in Google search results. This happens because Google takes a snapshot of each page and caches (stores) that version. It may take some time for Google to revisit the webpage to update its cache which is why your picture may continue to show up in Google results even though it's been removed from the website. You can submit a request to Google to have the cached page removed. Select "Remove outdated content" and follow the directions provided by Google.

3. **Submit a request to Google to remove the content:** If a nude or sexually explicit image or video has been shared without your consent and is appearing in Google search results, submit a report directly to Google.

Source: https://needhelpnow.ca/app/en/removing_pictures-facebook

It is advisable that the website is visited periodically to see if there are any updates and new information available.

Calling Helplines

Phone CHILDLINE 1098 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. CHILDLINE is a platform bringing together the MWCD, Department of Telecommunications, street and community youth, non-profit organisations, academic institutions, the corporate sector and concerned individuals.

Aarambhindia hotline: Go online to report child sexual abuse materials at the hotline hosted on **www.aarambhindia.org.** Report the URL of the image or video on the internet that shows sexual abuse of children through five steps online form. It is not necessary for the person who is reporting to identify himself or herself.

Aarambhindia draws upon the technological expertise of UK based Internet Watch Foundation (IWF) to determine the criminality and severity of the content (albeit against law in the UK) and the location from where it was uploaded and where it is being hosted. IWF thereafter initiates the

process of removing the offensive content with help from the law enforcement agencies and the hosting company. It also adds the offending URL to its comprehensive and frequently updated URL blocking list, which guides most major internet companies. In this way, further access to the content is disrupted until it is removed. Once the content is removed, the content is assigned a hash- a unique number generated from the data in the content that is to be used to identify, remove copies of the image/video and prevent future uploads.

Aarambhindia also provides assistance in the investigation of the case and rehabilitation of the child victim and family.

National Commission for the Protection of Child Rights, POCSO E-box: This is an initiative by NCPCR to help children report sexual abuse related offences directly to the Commission through this online complaint mechanism. The **POCSO e-box** is an easy and direct medium for reporting any case of sexual assault under Protection of Children from Sexual Offences {POCSO) Act, 2012. It is displayed prominently in the home page of NCPCR website visit http://www.ncpcr.gov, http://www.ncpcr.gov.in/index2.php where the user has to simply press a button named, **POCSO e-box** which will navigate to a page with the window having a short animation movie.

In telling children/complainant that it's not their fault and they need not have to feel bad. The NCPCR is their friend and will help them. This page will have an arrow button with "Press here". When pressed it will navigate to a page asking picture options. User has to select at least one option, fill the form and click on submit option to register the complaint. After this an acknowledgement that the complaint has been registered and a registration number will be displayed.

Contact the 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

Approach the school authorities

If your school has a counsellor, do not hesitate to discuss the problem you are facing with them. They are there to answer your questions, give guidance and assistance, as required.

Report to the police

Individuals (Children, parents or concerned adult/NGOs on their behalf) can approach 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. In case you are unable to file a complaint in the cyber cell, you can file an FIR with the local police station.

Filing an FIR

It is not necessary to know the name of the person responsible for the crime to lodge a FIR. Tell the police whatever you know.

You do not have to know all the details. Any anonymous communication, which constitutes criminal intimidation, can be punished under Section 507 of the IPC. It allows the victim to file a complaint without knowing the identity of the harasser.

Gather as much information as you can by taking screenshots of relevant messages, conversations and comments that can help your case.

A lot of the offenses mentioned above are cognizable, which means that the police can act, without waiting for the magistrate to issue a warrant.

The Protection of Children from Sexual Offences (POCSO) Act, 2012, also provides protection for boys and girls below 18 years who have experienced or are at risk of child sexual abuse, including sexual assault, sexual harassment, and making and selling child pornography.

Anyone who finds out or is suspicious that child sexual abuse is taking place is legally obliged to report it to the police. Failure to do so can invite penalties. The police is duty bound to make a written record of the complaint.

Special Courts try cases under the POCSO so that they are dealt with quickly. If the crime is proved, the offender is punished depending on the intensity and the act of sexual abuse. The punishment is enhanced if the offender is someone in a position of trust or authority. The courts may order compensation for the physical and mental pain suffered by the child.

Children and young people

Peer support

Parents and guardians

- Ask your children to tell you about the websites and apps they like to use and what they enjoy doing.
- Ask them about how they stay safe online. What tips do they have for you, and where did they learn them? What is okay and not okay to share?
- Ask them if they know where to go for help, where to find the safety advice, privacy settings and how to report or block on the services they use.
- Encourage them to help someone! Perhaps they can show you how to do something better online or they might have a friend who would benefit from their help and support.
- Think about how you each use the internet. What more could you do to use the internet together? Are there activities that you could enjoy as a family?

http://www.childnet.com/resources/supporting-young-people-online

Additional resources available at: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=1990313

http://blogs.lse.ac.uk/parenting4digitalfuture/2017/07/12/friends-like-me-the-screen-lives-of-children-and-teens/

What can I do right now?

- Make sure that you have an open dialogue with your child and encourage them to talk to you about their internet use: for example, who they're talking to, services they're using, and any issues they may be experiencing.
- Create a family agreement to establish your children's boundaries, and your expectations, when on the internet.
- Give your child strategies to deal with any online content that they are not comfortable with – such as turning off the screen, telling an adult they trust and using online reporting facilities.
- Consider using filtering software to block unwanted content. In addition to filtering, remember that discussion with your child, and involvement in their internet use, are both effective ways to educate them about the internet.
- Encourage your children to 'think before you post.' Online actions can impact not only yourself but the lives of others. Content posted privately online can be publicly shared by others, and may remain online forever.
- Understand the law. Some online behaviour may break the law, for example when downloading or sharing content with others. Be able to recommend legal services.
- Familiarize yourself with (i) privacy settings; (ii) reporting features available on popular sites and services; (iii) the age ratings for games and apps which indicate the level and suitability of the content. Also see if online reviews are available from other parents as these may be helpful.
- Save all the available evidence if your child is being bullied online and know where to report the incident, for example to the school, service provider, or the police if the law has been broken.
- Set up a family email address that your children can use when signing up to new games and websites online.
- Encourage your children to use nicknames (where possible) instead of their full name online, to protect their personal information, and create strong passwords for every account.

Set up a PIN or password on devices to help protect personal information.

Educating the REPORTING TOOLS with Examples on various popular platforms of Web and Mobile. How to Report, where to report with examples.

School authorities

- Reporting mechanism needs to be in place with well-defined roles and responsibilities
- Capacities of counsellors updated to include skills for dealing with online safety of children
- All children should be aware of these mechanisms

Police

- Cyber cells at police stations need to be in place and adequately resourced
- Capacities of staff need to be updated to understand fully the range of online offences against children and child-sensitive ways of dealing with children to record complaints
- Contact details of the cyber cell need to be advertised widely so all people know whom to contact, if required

4. Seeking Help

Discussing online experiences with friends and trusted adults

If you are worried about something that is happening to you or a friend, seek help. Talking about the problem can be the first step to solving it. Talk to an adult who you trust like a parent, caregiver or a teacher about what is happening. Talking about a problem can often make you feel better. If you keep your worries to yourself they can grow and grow inside. It is a lot easier to solve a problem when there are two heads working together on it.

But it is not always easy to know how to start the conversation. 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 isn't 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.

Seeking technical assistance

When technical assistance can help?

1. When accounts are hacked and need to be recovered
2. Any virus attack on device
3. To report violating (abusive? Offensive?) content (and fraud?)
4. When simple filters /tools are required to protect young children from inappropriate content, blocking adult/ inappropriate content websites

Where to seek assistance?

#1 Draw upon processes put in place by social media companies to address inappropriate and abusive content on their sites, and they are expected to respond quickly to incidents of abusive behavior on their networks.

Check out information about their safety and privacy policy on their sites

Technical assistance: This section is being worked out and will be incorporated shortly in the online version.

Seeking counselling and psycho-social support

When excessive use of devices is harming health and well-being?

Recognize the "dangers" of excessive use

Review the following statements and answer in "yes" or "no" if they describe your current situation:

- I have continuous desire to use (craving)
- I am not able to reduce the use (control)
- I use it to feel relax or to manage mood swing (coping)
- I have a strong urge to use (compulsion)

- I postpone my sleep for internet use (consequences)

Presence of four "yes" or more indicates the need to disconnect from Internet and to reconnect with others.

Stress due to online experiences

It does not matter whether abuse happens online or offline, a child can experience harm and long-lasting damage as a result of harassment and abuse (e.g. bullying, "inappropriate" content, undue attention from strangers,)

Cyberbullying like bullying can cause school failure, depression, anxiety and other mental health problems. Indeed, it can make children and young people feel more frightened and helpless than bullying because they feel like they cannot escape.

Not much is known as yet about the effects of grooming or sexual abuse experienced online but there is sufficient evidence of the devastating effects of sexual abuse that can last into adulthood. The effects of bullying can last into adulthood and, at its worst, it has driven children and young people to self-harm, including suicide. All children who are affected by bullying can suffer harm – whether they are bullied, they bully others or they witness bullying.

Children who are bullied are more at risk of developing mental health problems, including depression and anxiety. Children at the highest risk are those who are both bullied, and who bully others.

Children who are bullied also:

- have fewer friendships
- aren't accepted by their peers
- are wary and suspicious of others
- have problems adjusting to school, and don't do as well.

Effects on children who witness bullying:

- become reluctant to go to school
- be frightened or unable to act
- feel guilty for not doing anything to help.

Sexual exploitation can be devastating for a child or young person with effects lasting throughout their lives. Although every child and situation is different, the following are some of the problematic outcomes:

- isolation from family and friends
- teenage parenthood
- failing examinations or dropping out of school altogether
- unemployment
- mental health problems
- suicide attempts
- alcohol and drug addiction
- aggressive behavior
- criminal activity.

Audience-specific information

Children

- Seek help if you are worried about something that is happening to you or a friend. Discussing the problem with a trusted adult (e.g., a parent, caregiver or a teacher) is the first step to solving it.
- If something is bothering you about your experience with use of technology you must share the concern with someone you can trust. This could be your parents, peers or teachers or school counselor.
- Your parents, teachers and counselor are there to help you. To understand your problem and find a solution and guide and support you and if required, advise you to meet a specialized person who will help you understand your problem and work a way out of it.
- Your friend or peers can share similar experiences they may be facing and inform you of how they sought help and advise.
- Sometimes sharing itself can help the anxiety or fear you may be facing and improve the situation. Also trying to cope with problems alone may not yield the appropriate actions from lack of accurate information about available help options.

Parents

- Be communicative and friendly with your children. Build trust and confidence that you are there for them, they can share whatever problems they may be facing, and you will support and help them.
- Keep yourself informed of how you can help your children and where you can seek help, if required.
- Recognize excessive use of devices amongst children and take appropriate and timely action.

Are today's children "addicted" to technology?

From smartphones to social media to video-games, media and technology have become integral to our lives. The ability to be connected constantly can affect schoolwork, relationships and concentration. How to get the most from technology without letting it get out of control is a challenge.

Many children use their phones or computers all the time, mostly to connect with friends. But it can become problematic when it gets in the way of other important activities, such as school and family time. If children are having problems keeping up with schoolwork, chores, and activities, help them get back on track with some limits. If they cannot control themselves -- they sneak their phones, feel bad about their behavior, lose friends, or stop other activities including schoolwork -- they may be showing signs similar to addiction. In either case, establishing and reinforcing a balanced approach to media may help. But you may want to talk to your pediatrician/ psychiatrist for more help.

Technology addiction and problematic use might look similar but are different. There is currently no universally acceptable definition of technology addiction. When people are addicted, their brains and bodies do not let them stop using or engaging in something even when it hurts them. Problematic media use may cause difficulties but limits can help.

School administrations

- Develop standards and guidelines for safe use of technology in schools, including roles and responsibilities for supervision and guidance of children, and advise parents to follow similar guidelines for use of devices at home.
- Ensure capacity of teachers and counselors in guiding the use of technology, dealing with all aspects of online safety for children and responsible use. They need to have skills to observe and guide students and advise parents. If problems persist or magnify, there may be a need to consult a psychiatrist for more help.
- Establish a system of referring students to appropriate services

Teachers

- Make children feel comfortable and confident about discussing their problems with you by being communicative and non-judgmental
- Update yourself regularly with latest safety measures, where to seek help or report problems
- Maintain a dialogue with parents. Pay attention when parents report the following in children to detect potential excessive use signs:
- Increasing and persistent use of the device, leading to social withdrawal
- Frequent requests to use the device, resulting in temper tantrums when the request is denied or the device is taken away
- Disengagement from activities, such as insisting to go home to use the device and refusing to perform other usual daily routines (such as going to bed) to continue playing with the device, not paying attention to studies/homework, not socializing with peers
- Excess preoccupation with certain characters found in games or videos, or spending excessive amounts of time and resources on them.

Police

- Update staff capacities and competencies for understanding and responding the ever-expanding range of online offences against children and child-sensitive ways of dealing with children to record complaints
- Put in place efficient and effective structures and services for reporting online offences
- Undertake awareness activities in schools on a regular basis.

Glossary

Internationally recognized terminology related to child online safety

Child sexual abuse materials:[19] The term "child sexual abuse material" is increasingly being used to replace the term "child pornography". This switch of terminology is based on the argument that sexualized material that depicts or otherwise represents children is indeed a representation, and a form, of child sexual abuse, and should not be described as "pornography".

Pornography is a term primarily used for adults engaging in consensual sexual acts distributed (often legally) to the general public for their sexual pleasure. Criticism of this term in relation to children comes from the fact that "pornography" is increasingly normalized and may (inadvertently or not) contribute to diminishing the gravity of, trivializing, or even legitimizing what is actually sexual abuse and/or sexual exploitation of children. Furthermore, as with the terms discussed above, "child prostitution" and "child prostitute", the term "child pornography" risks insinuating that the acts are carried out with the consent of the child, and represent legitimate sexual material.

So called "child pornography" *"involves children who cannot (legally) consent"* to the sexual acts they are being subjected to, *"and who may be victims of a crime"*. This has been the general approach of the law enforcement sector in recent years, and it has led the way in characterizing "child pornography" as forensic evidence of the sexual abuse or exploitation of children.

Today, most child sexual abuse/exploitation material is exchanged, bought, and sold online, making the online dimension of this crime almost omnipresent.

The term "child sexual abuse images" has also sometimes been used in this context. However, it is important to note that, by limiting the terminology to "*images*", the risk exists of excluding other forms of material representing child sexual abuse and exploitation, such as audio files, written story lines, or other potential forms of recording. Therefore, many child protection organizations as well as law enforcement agencies working on these issues today prefer the term "material" to "images".

Cyber bullying:[20] While bullying typically happens at school or work, cyberbullying takes place over cyberspace. This includes both Internet and cell phone communication. Like physical bullying, cyberbullying is aimed at younger people, such as children and teenagers. It may involve harassing, threatening, embarrassing, or humiliating young people online.

Cyberbullying can take many forms, including:

- Making fun of another user in an Internet chat room.
- Harassing a user over an instant messaging session.
- Posting derogatory messages on a user's Facebook or MySpace page.
- Circulating false rumors about someone on social networking websites.
- Publishing lewd comments about another person on a personal blog.
- Posting unflattering pictures of another user on the Web.

[19] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/
[20] https://techterms.com/definition/cyberbullying

- Spamming another user with unwanted e-mail messages.
- Sending threatening or provocative e-mails.
- Repeatedly calling another person's cell phone.
- Sending unsolicited text messages to another user.

Cyber stalking:[21] Technically, cyberbullying takes place between two young people. When adults are involved, it may be called cyber-harassment or cyberstalking.

Cyber predation:[22] A Cyber predator uses the Internet to hunt for victims to take advantage of ANY way, including sexually, emotionally, psychologically or financially. Cyber predators know how to manipulate children, creating trust and friendship where none should exist.

Digital footprint: The trail of data left, including the websites visited, the emails sent, and information submitted to online services, by every user of the Internet is known as digital footprint. It is active when the data is intentionally submitted online, for instance, by sending emails, publishing a blog, posting social media updates, and generally spending more time on social networking websites. The user expects the data sent through the email to be seen and/or saved by another person. Since most people save their email online, the messages they send can easily remain online for several years or more. Every tweet posted on Twitter, every status update or "like" on Facebook, and every photo shared on Instagram contributes to the user's digital footprint. However, it is passive when the data trail is left online unintentionally. When a user visits a website, the web server logs his/her IP address, which identifies his/her Internet service provider and approximate location. While the user's IP address may change and does not include any personal information, it remains part of his/her digital footprint. Some search engines also save search histories when the users are logged in.

Exploitation of children in/for prostitution:[23] "Sexual exploitation of children in/for prostitution" is frequently referred to as "child prostitution", in recent legal instruments and in mass media. Performance of a sexual act by a child in exchange for, or a promise of, something of value (money, objects, shelter, food, drugs, etc.).

Usually a third person rather than the child receives the object of exchange. The object of exchange may not actually be given; the mere promise of an exchange suffices, even if it is never fulfilled.

Grooming:[24] Building an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. Children and young people can be groomed online or face-to-face, by a male or female stranger or by someone they know. Many children and young people do not understand that they have been groomed or that what has happened to them is a form of abuse. They may tend to feel that what is developing between them and the perpetrator is a 'relationship'.

Live online child sexual abuse:[25] The terms such as "streaming" and "webcam" merely describe a

[21] https://techterms.com/definition/cyberbullying
[22] http://cybersafetycsusm.weebly.com/cyber-predators.html
[23] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/
[24] NSPCC
[25] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/

technological means that take into account neither the intention of the perpetrator nor the result of the committed acts—namely, the sexual abuse and/or exploitation of a child.

Instantaneous transmission of child sexual abuse imagery to viewers through "streaming" over the Internet. Importantly for the viewer, streaming leaves no trace on the device, because no file is downloaded. When the streaming stops the child sexual abuse material disappears unless it is recorded by the offender. This increases the perception of impunity of the offender, and creates specific challenges for post-event investigation, particularly relating to the recovery of evidence and the identification of victims and offenders.

Online child sexual exploitation:[26] The terms "ICT-facilitated" and "cyber-enabled" child sexual exploitation are sometimes used as alternatives to define these practices.

The use of Internet as a means to exploit children sexually.

The reference to "online child sexual exploitation" includes all acts of a sexually exploitative nature carried out against a child that have, at some stage, a connection to the online environment. It includes any use of ICT that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted. This notion can thus encompass (but is not limited to):

- sexual exploitation that is carried out while the victim is online (such as enticing/ manipulating/ threatening a child into performing sexual acts in front of a webcam
- identifying and/or grooming potential child victims online with a view to exploiting them sexually (whether the acts that follow are then carried out online or offline)
- the distribution, dissemination, importing, exporting, offering, selling, possession of, or knowingly obtaining access to child sexual exploitation material online (even if the sexual abuse that is depicted in the material was carried out offline)

Pharming:[27] Manipulation of users by hackers on the Internet by redirecting them to false websites without their knowledge.

While a typical website uses a domain name for its address, its actual location is determined by an IP address. When a user types a domain name into his or her Web browser's address field and hits enter, the domain name is translated into an IP address via a DNS server. The Web browser then connects to the server at this IP address and loads the Web page data. After a user visits a certain website, the DNS entry for that site is often stored on the user's computer in a DNS cache. This way, the computer does not have to keep accessing a DNS server whenever the user visits the website.

Pharming can take place via an e-mail virus that "poisons" a user's local DNS cache. It does this by modifying the DNS entries, or host files. For example, instead of having the IP address 17.254.3.183 direct to www.apple.com, it may direct to another website determined by the hacker. When entire DNS servers are infected, any user that uses the affected DNS server will be redirected to the wrong website. Many people are affected at once when the DNS server that is

[26] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/
[27] https://techterms.com/definition/pharming

modified by pharming is large. Most DNS servers have security features to protect them against such attacks but they are not always immune as hackers continue to find ways to gain access to them.

Phishing:[28] Phishing is a fraud used by scammers or hackers to collect personal information from unsuspecting users. They send out emails that appear to come from legitimate websites seeking updating or validation of information and require the users to enter their username and password, after clicking a link included in the e-mail. Some e-mails ask additional information (e.g., full name, address, phone number, and credit card number). Once the user visits the false website and enters username and password, the phisher may be able to gain access to more information by just logging in to the account. The false emails often look rather legitimate, and even the Web pages where the user is directed to may look real.

Sexting:[29] **"**Self-production of sexual images" or as the "exchange of sexual messages or images" and "the creating, sharing and forwarding of sexually suggestive nude or nearly nude images through mobile phones and/or the internet" is known as sexting. Sexting is a form of self-generated sexually explicit content, and the practice is "remarkably varied in terms of context, meaning, and intention"

"Sexting" is possibly the most common form of self-generated sexually explicit content involving children, and is often done by and among consenting adolescents who derive pleasure from the experience. There are also many forms of "unwanted sexting". Non-consensual sexting includes sharing or receiving unwanted sexually explicit photos, videos, or messages, for instance by known or unknown persons trying to make contact, put pressure on, or groom the child. Sexting can be a form of sexual bullying, where a child is pressured to send a picture to a boyfriend/ girlfriend/ peer, who then distributes it to a peer network without their consent.

Trolling:[30] Posting of offensive, incendiary, or off topic comments online – on Web forums, Facebook, chatrooms, and after news articles or blog entries. This activity is highly discouraged and may constitute a violation of the online community's user agreement.

URL: "Uniform Resource Locator", commonly known as a URL is the unique location or address of a specific webpage or file on the Internet.

Virtual child sexual abuse:[31] "Virtual" relates to online artificially or digitally created images of children involved in sexual activities. The realism of such images creates the illusion that children are actually involved, although this is not the case. The term "online child sexual abuse" is widely used to refer both to the sexual abuse of children that is facilitated by ICTs (e.g. online grooming) and to sexual abuse of children that is committed elsewhere and then repeated by sharing it online through, for instance, images and videos. The preferred term in the case of the former is "online-facilitated child sexual abuse".

Sextortion:[32] Sexual extortion, also called "sextortion", is the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favors, money, or other

[28] https://techterms.com/definition/phishing
[29] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/
[30] https://techterms.com/definition/troll
[31] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/
[32] Luxembourg Guidelines Terminology. Available at: http://luxembourgguidelines.org/english-version/

benefits from her/him under the threat of sharing the material beyond the consent of the depicted person (e.g. posting images on social media). Often, the influence and manipulation typical of groomers over longer periods of me (sometimes several months) turns into a rapid escalation of threats, intimidation, and coercion once the person has been persuaded to send his or her sexual images.

Sexual extortion is considered a feature of online solicitation of both children and adults, and there appears to be an increase of the use of this type of blackmailing, including more extreme, violent, sadistic, and degrading demands by offenders. When carried out against children, sexual extortion involves a process whereby children or young people are coerced into continuing to produce sexual material and/or told to perform distressing acts under threat of exposure to others of the material that depicts them. In some instances, the abuse spirals so out of control that victims have attempted to self-harm or commit suicide as the only way of escaping it.

References

Livingstone, S., and Bulger, M. (in press) A global research agenda for children's rights in the digital age. Journal of Children and Media

Jaishankar and Halder, Cyber Crimes against Women, 2017;

Seth, Karnika, Protection of Children on the Internet, 2015

Useful websites

www.aarambhindia.org

http://www.bbc.com/news/education-38508888

http://www.ceop.police.uk

http://www.childnet.com/resources/trust-me?utm_content=buffera424c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

http://www.childnet.com/ufiles/Family-agreement-advice.pdf

http://www.childnet.com/ufiles/Guidance-for-teachers1.pdf

http://www.childnet.com/ufiles/Family-agreement-advice.pdf

http://www.childnet.com/ufiles/Guidance-for-teachers1.pdf

http://cybersafeindia.org/cyber-safety-kids.html

http://cybersafeindia.org/cyber-safety-parents.html

http://cybersafeindia.org/cyber-safety-teachers.html

http://cybersafeindia.org/cyber-safety-citizens.html

http://www.digitalcitizenship.net/Nine_Elements.html

https://dmlcentral.net/trouble-screen-time-rules/#.WM0LvRzwf1c.twitter

http://www.infosecawareness.in

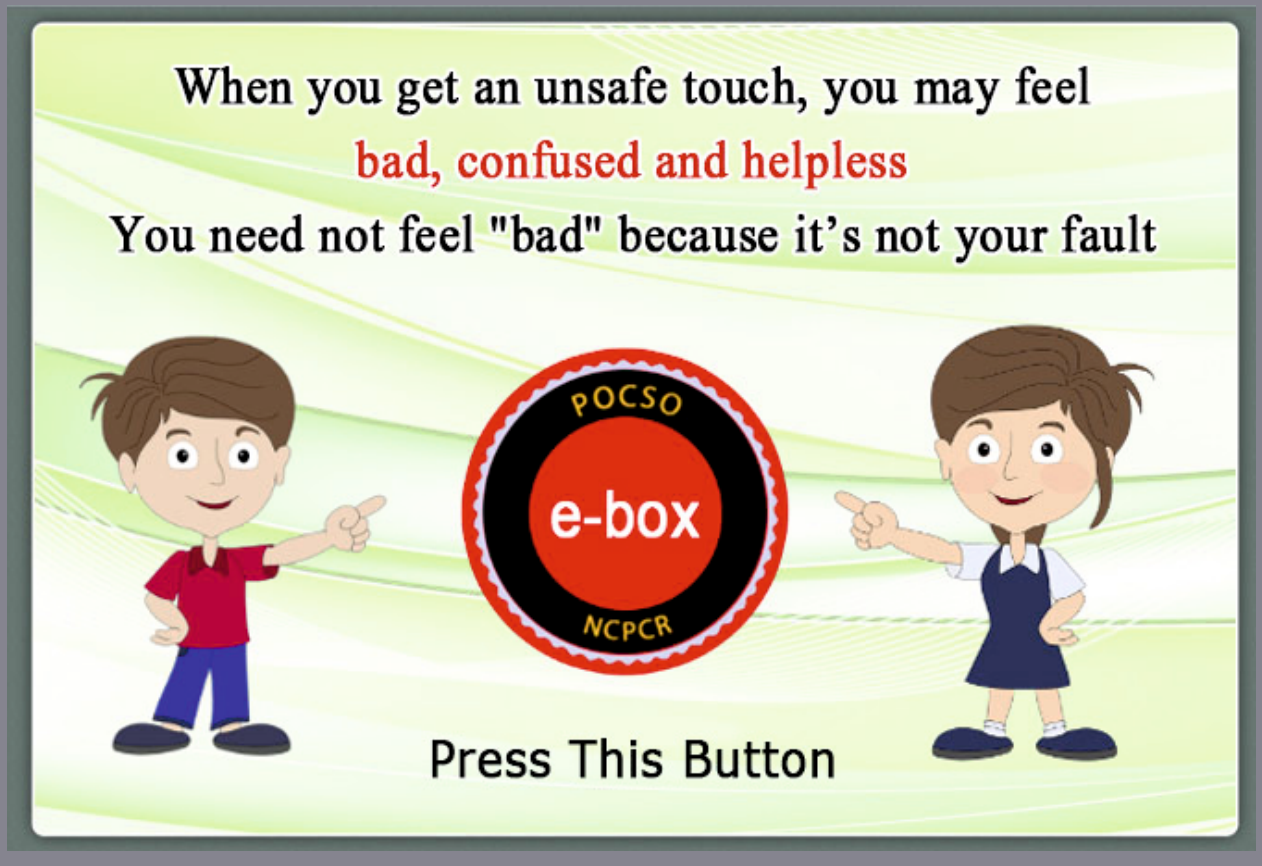
http://www.iwf.org.uk

http://luxembourgguidelines.org/english-version/

http://www.netsmartz.org/Parents

http://www.netsmartz.org/Educators

http://www.unicef.in/StaySafeOnline/index.html



National Commission for Protection of Child Rights (NCPCR)
5th Floor Chanderlok Building, 36 janpath, New Delhi 110001
Phone: 011-23478200
Pocso e-box No. -9868235077
Visit http://www.ncpcr.gov.in
Follow us @NCPCR_
Like us /NCPCR.Official