Directorate of Education
Govt. of NCT of Delhi

Cyber

NISHTHA

Guidelines on Cyber Safety for Adolescents

CONTENTS

Foreword 3

Acknowledgment 4

Importance of Cyber NISHTHA Guidelines 5

About Cyber NISHTA Guidelines 6

Drafting Committee 7

Glossary 8

Part – A: Context Setting 11

I. Introduction 11

II. Why are online risks against adolescents? 13

III. Forms of online risks against adolescents 14

IV. What is Online Safety? 16

Part – B: Legal & Policy Framework 18

I. Legal & Policy Framework 19

Part – C: Guidelines and Standard Operating Procedures 21

I. About the Guidelines & Standard Operating Procedures 22

Part – D: Understanding and Preventing Online Risks 24

I. Cyberbullying 25

II. Online Grooming 28

III. Data Privacy Breaches 31

IV. Hacking and unauthorized access 34

V. Cyberstalking 37

VI. Non-Consensual Sharing of Images 40

VII. Child Sexual Exploitation and Abuse Material (CSEAM) 43

VIII. Deepfakes (AI-Generated Fake Media) 46

IX. Addiction to Gaming Platforms 49

X. Digital Payments Scam 52
XI. In-App Purchases 55
XII. Call Bombing 58
Part – E: Device Related Risks 61
I. Phishing 62
II. Stalkware 63
III. Ransomware 64
IV. Malware Attack 65
Part F: Responsibly using AI Tools 66
Part G: Cyber-Safe Design Standards for School Apps and Portals 71
Part H: Annual Cyber Safety Mock Drill Plan 74
Part I: Roles & responsibilities of stakeholders 80
I. Institutional Mechanisms and Action Points for Online Safety of Adolescents 81
II. Procedure for Response to Online Incidents 83
Annexures 87
References 100

FOREWORD

In today's digital age, technology has become an inseparable part of children's lives — shaping the way they learn, communicate, and explore the world. While the internet offers limitless opportunities for education and innovation, it also brings with it new and complex challenges that threaten the safety, privacy, and wellbeing of our students. The growing cases of cyberbullying, online grooming, body shaming, identity theft, and exposure to harmful content remind us that digital spaces must be made as safe as our classrooms.

Recognizing this urgent need, the Directorate of Education, Government of NCT of Delhi,in association with Matri Sudha and its national collective Cyber Chakravyuh, has developed the Cyber NISHTHA (N – Navigate Safely; I – Identify Risks Early; S – Safeguard Privacy; H – Help-Seeking Behaviour; T – Think Before You Click; H – Healthy Digital Habits; A – Act Responsibly) Guidelines and Cyber Yodha Ambassadors Module on Cyber Safety of Adolescents in Delhi to empower schools, students, teachers and parents to Stay Safe Online!

This initiative aligns with the vision of the National Education Policy (NEP) 2020 and national child protection frameworks such as the POCSO Act, IT Act, and Bhartiya Nyaya Sanhita, emphasizing the collective responsibility of educational institutions to ensure that technology becomes a tool for empowerment, not exploitation.

I call upon all schools to adopt these guidelines in letter and spirit, to conduct regular cyber safety awareness programmes, and to build systems for reporting and responding to online risks. Together, we can ensure that every child in Delhi grows up digitally smart, emotionally secure, and confidently equipped to face the opportunities and challenges of the cyber world.

(Veditha Reddy, IAS)
Director
Directorate of Education & Sports
Government of NCT of Delhi

ACKNOWLEDGMENT

The Directorate of Education, Government of NCT of Delhi, expresses its gratitude towards Ms. Veditha Reddy, Director, DoEfor expressing her commitment to the cause of cyber safety of adolescents.

The Directorate gives its sincere appreciation to Sh. Arvind Singh, Director, Matri Sudha and its national collective Cyber Chakravyuh, who led the process in preparation of Cyber NISHTA Guidelines. His extensive grassroots experience with expertise in policy development through strategic partnerships with government institutionshave been instrumental in developing this comprehensive document.

The Directorate acknowledges Ms. Seema Roy Chowdhury, Deputy Director, EVGB who anchored the multi-stakeholder consultation for the development and preparation of the guidelines. Ms. Upasna Khatri, CIC, South; Ms. Malvika Joshi, Ms. Gitika Kohli, Mr. Ankur Dahiya, Ms. Rashika Badgujar (EVGC) Ms. Swati Sharma, Counsellor-Incharge, EVGB for coordination and reviewing the document.

The Directorate acknowledges Sh. Manoj Kumar (ACP), IFSO, Cyber Crime, Delhi Police, for his valuable contribution in development and preparation of this document.

The Directorate acknowledges individual expert's (Dr. Priyanka Kochar, Adolescent Health Expert; Dr. Vikram Srivastava, Founder, Independent Thought; Ms. Vidhu Prabha, Country Lead, Rise Up Together; Ms. Sakshi Rewaria, Faculty of Law, IIM, Rohtak, Haryana; Mr. Ravi Shanker Rai, Sr. Programme Manager, Matri Sudha) efforts in online risks, understanding adolescents' digital behaviour, and proposing practical school-based interventions have significantly enriched the content and direction of these guidelines.

This collaboration reflects our shared vision of ensuring that every adolescent in Delhi is empowered with the knowledge, resilience, and confidence to use digital technology safely and responsibly.

We look forward to continued cooperation with all stakeholders in making Delhi's schools models of cyber awareness and digital wellbeing.

(Dr. Patil Pranjal Lahensingh, IAS)
Additional Director of Education
Directorate of Education, Govt. of NCT of Delhi

IMPORTANCE OF CYBER NISHTHA GUIDELINES

EVGB, Directorate of Education, GNCTD in partnership with Matri Sudha, brought together key stakeholders including senior officials, cyber safety experts, educators, and school counsellors to deliberate on strengthening digital safety among adolescents in schools, which led to the development of the guidelines.

I would like to express my sincere gratitude to our Honourable Director, Ms. Veditha Reddy; the Honourable Additional Director, Dr. Pranjal Patil Lahensingh; and the entire EVGB team for their tireless efforts in producing this work.

A key benefit of these guidelines is the promotion of responsible online behaviour. Students learn about digital etiquette, respect for others in online interactions, and the consequences of misuse of technology. This contributes to the development of a disciplined and respectful digital culture within and beyond the school environment.

The guidelines aim to build foundational awareness among students regarding safe and ethical use of digital technologies. These guidelines equip students with essential knowledge about protecting personal information, recognizing cyber threats, and responding appropriately to suspicious online activities. By fostering digital literacy, students are empowered to make informed decisions in the virtual space.

Moreover, integrating Cyber NISHTHA into the school ecosystem supports the development of critical thinking and digital responsibility among students. It prepares them to become informed digital citizens who can safely navigate the online world while contributing positively to society.

In conclusion, the guidelines are instrumental in ensuring student safety, enhancing digital competence, and promoting responsible use of technology.

(Seema Roy Chowdhury)
Deputy Director of Education
EVGB, Directorate of Education, Govt. of NCT of Delhi

ABOUT CYBER NISHTHA GUIDELINES

Today, that world is deeply digital, the children and adolescents learn quickly how to enter it: creating social media accounts, playing online games, sharing photographs, and forming digital friendships. But very often, they are not taught how to navigate its risks or how to exit dangerous situations.

The internet opens doors to learning, creativity, friendship, and opportunity. Yet, alongside these possibilities, there are risks that children and adolescents often face silently—cyberbullying, manipulation, exploitation, and emotional harm that can travel through screens into their everyday lives.

Under the able guidance of Ms. Vedita Reddy (IAS), Director, Directorate of Education, Ms. Patil Pranjal Lahensingh (IAS), Additional Director, Ms. Seema Roy Chowdhary, Deputy Director, EVGC, Directorate of Education, this robust work in the form of cyber safety guidelines is undertakenin the best interest of children and adolescents in NCT of Delhi.

From a governance perspective, the adoption of the Cyber NISHTA Guidelines represents a defining moment in Delhi's policy journey.By institutionalizing digital safety within the education ecosystem, Delhi has the opportunity to become the first state in India to treat adolescent cyber safety as a core element of educational governance and child protection. Such a step would not only safeguard millions of young digital citizens but also set a national precedent for responsible digital governance.

Arvind Singh
Director, Matri Sudha
Co-Founder, Cyber Chakravyuh

DRAFTING COMMITTEE

The drafting committee of Cyber NISHTHA: Guidelines on Cyber Safety for Adolescents in NCT of Delhi constituted the following members:

S. No.	Name	Institution
1.	Ms. Veditha Reddy (IAS)	Director, Directorate of Education & Sports, Govt. of NCT of Delhi
2.	Dr. Patil Pranjal Lahensingh	Additional Director, Directorate of Education & Sports, Govt. of NCT of Delhi
3.	Ms. Seema Roy Chowdhury	Deputy Director, EVGB, Directorate of Education, Govt. of NCT of Delhi
4.	Sh. Manoj Kumar	Assistant Commissioner of Police (ACP), IFSO, Cyber Crime, Delhi Police
5.	Arvind Singh (Adv.)	Director, Matri Sudha & Co-Founder, Cyber Chakravyuh
6.	Dr. Priyanka Kochar	Technical Expert, Adolescents Health
7.	Dr. Vikram Srivastava (Adv.)	Founder, Independent Thought & Co-Convener, Cyber Chakravyuh
8.	Vidhu Prabha	India Country Lead, Rise Up Together
9.	Mr. Ravi Shanker Rai	Sr. Programme Manager, Matri Sudha
10.	Ms. Swati Sharma	Counsellor-Incharge, EVGB, Directorate of Education, GNCTD
11.	Ms. Upasna Khatri	CIC, South, Directorate of Education, GNCTD
12.	Ms. Malvika Joshi	EVGC, EVGB, Directorate of Education, GNCTD
13.	Ms. Gitika Kohli	EVGC, EVGB, Directorate of Education, GNCTD
14.	Mr. Ankur Dahiya	EVGC, EVGB, Directorate of Education, GNCTD
15.	Ms. Rashika Badgujar	EVGC, EVGB, Directorate of Education, GNCTD
16.	Sakshi Rewaria (Adv.)	Faculty of Law, IIM, Rohtak, Haryana

GLOSSARY

Antivirus Software: A program that protects computers or phones from malicious software (malware) by finding and blocking viruses and worms.

Blocked: A feature that stops someone from messaging you or viewing your profile online.

Call-Filtering: Settings that help reduce or stop calls from unknown or unwanted numbers.

Childline 1098: A 24×7 toll-free helpline for children in distress in India.

Child Welfare Committee: CWCs exist in each district or for a group of districts and act as the final authority for children in need of care and protection.

Cybercrime: Any illegal act involving computers, networks, or the internet (e.g. hacking, fraud, spreading malware).

Cyber Police: The police officers who protect people on the internet. They help stop online bullying, hacking, cheating, and people who try to harm others using computers or phones.

Delhi Commission for Protection of Child Rights (DCPCR) is a statutory body which help and protect children living in Delhi.

Digital Citizen: A person who uses technology and the internet in a safe, respectful, and responsible way.

Digital Footprint: All the information and content (posts, photos, comments, search history) that someone leaves behind when they use the internet.

Digital Literacy: It means knowing how to find information online, use social media responsibly, and recognize safe vs. unsafe content.

Digital Personal Data Protection Act (DPDP Act) 2023: It explicitly treats children (under 18) as a sensitive category, requiring verifiable parental consent before collecting or using a child's personal data.

Digital Well-being: Taking care of physical, mental, and emotional health while using technology.

Ethical Hacking: Itmeans using computer and internet skills in a legal and responsible way to help keep systems safe.

Inappropriate Content: Online material that is not suitable for children and may make them feel uncomfortable, scared, or confused.

In-App Purchase: Money spent inside an app or game to buy extra items, features, or levels.

Information Technology (IT) Act, 2000: It defines offenses like hacking, cyber pornography, and online fraud, and sets penalties for them.

Misinformation: False or incorrect information shared without knowing it is untrue.

The National Commission for Protection of Child Rights (NCPCR) is a statutory body which works to keep children safe, healthy, and happy.

The National Commission for Women (NCW) is a statutory body which work to keep women and girls safe and respected.

Online Safety: Rules and habits that help protect people from harm while using the internet.

OTP (One-Time Password): A secret code sent to a phone or email to confirm a payment or login. It should never be shared with anyone.

Parental Controls: Tools or app/settings that allow parents to restrict what children can see or do on devices.

Parental Consent (Digital): It's meant to ensure parents know what data about their child is being used and can protect the child's privacy.

PIN: A personal secret number used to access bank accounts or payment apps.

Pop-up: A message or screen that suddenly appears while using an app or game.

POCSO e-box: This is meant to aid you to register any case of sexualharassment of a child victim (including online abuse). You can enter details as instructedon the e-box web page: https://ncpcr.gov.in/pocso/public/

Privacy: The right to keep personal information, photos, and messages safe and private.

Privacy Settings: Controls on apps or websites that help you decide who can see your posts and contact you.

Screenshot: A picture taken of the screen to save messages or posts as evidence.

Screen Time: The amount of time spent using digital devices such as phones, tablets, computers, or gaming consoles.

Social media: Online platforms (like Facebook, Instagram, WhatsApp, YouTube, etc.) where people create profiles, share content, and connect.

Trusted Adult: A parent, teacher, school counsellor, or guardian who can help you if something online feels wrong.

Trusted Source: A reliable person or organisation that provides correct information, such as teachers, parents, schools, or official news platforms.

Two-Factor Authentication (2FA): An extra security step when logging into an account. Use 2FA on email, social media, banking, and other important accounts for better protection.

Unethical hacking: It means using computer or internet skills to enter someone else's account, device, or data without permission.

Unknown Number: A phone number that is not saved in your contacts.

CONTEXT SETTING

PART – A : CONTEXT SETTING

I. Introduction

Imagine a place bigger than the biggest city in the world—a place where you can explore countries without moving, learn fun facts, play games, and chat with friends whenever you want. This amazing world is called cyberspace, and we use it every day to study, play, and discover new things. But just like any big city, the internet has rules, and we must stay alert and make smart choices to stay safe while enjoying all the exciting things it offers.

In India, and especially in Delhi where so many young people use the internet, technology has changed the way children, adolescents and youths learn and connect with others. Easy access is great, but it also means more people go online without knowing how to protect themselves. The internet gives amazing chances to learn and express yourself, but it can also expose adolescents to hidden risks. That's why understanding online safety is so important[1] .

Today, almost everyone uses social media—Facebook, Instagram, WhatsApp, Snapchat, X, YouTube—to share photos, stories, and messages. It's like a huge global playground where you can meet new people, learn about different cultures, and stay connected with family and friends. But just like any playground, you must stay careful because not everyone online is kind or safe. For adolescents, social media offers

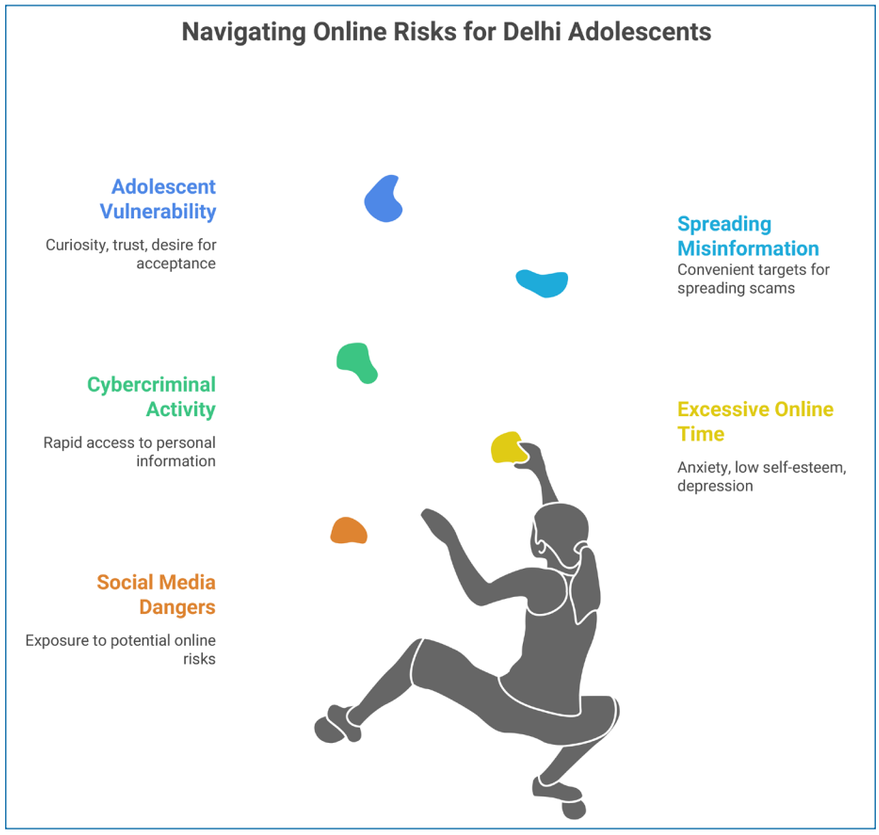


Figure 1: Navigating Online Risks

[1]Are Adolescents Equipped for Breaking the Cyber Chakravyuh, Matri Sudha, 2025.

- **Internet Usage: As of 2025, 98.3% male and 97.4% female aged 15–29 years in Delhi used the internet. (Comprehensive Modular Survey: Telecom, 2025)**
- **Internet Connections per Capita: In 2023, Delhi distinguished itself further with an astonishing 187 internet connections per 100 persons, far ahead of the national average of ~60 per 100. (State of India's Digital Economy Report, 2023)**
- **Tele-density Leader: A 2021 NITI Aayog report showed Delhi led with 199.9 internet subscribers per 100 population and a mobile tele density of 190.6 per 100.**
- **Top Tele-density in 2023: Delhi reached a remarkable 276.8 phones per 100 people, as per TRAI data—highlighting more active SIMs than residents.**
- **"Elite" Status Since 2008: Delhi has maintained over 100% mobile penetration for many years, symbolizing deep market saturation. (TRAI)**

many opportunities for connection and self-expression, but it also brings risks. Spending too much time online can lead to anxiety, low self-esteem, and depression, especially for those who depend heavily on likes and comments for validation. Many young people also experience “Fear of Missing Out” (FOMO), feeling left out when they see others having fun without them. This can lead to compulsive checking, reduced focus on studies, and weaker real-life relationships.

Still, when used in moderation, social media can provide support and community. Online groups can help adolescents connect with peers and access resources, including mental health information. As Best et al. (2014) note, social media can encourage positive interaction—but balanced, mindful use is essential.

Cyber criminals target social media and other online platforms because they offer rapid access to large volumes of personal information and facilitate interactions with a broad audience. The ease of sharing and the openness of digital platforms make them convenient targets for spreading misinformation, scam messages, or malicious software. Adolescents, in particular, may be vulnerable to these tactics due to curiosity, trust in online relationships, or the desire for social acceptance.These factors combine to create the "Cyber Chakravyuh"— for creating a unified effort in education, awareness generation, enforcement and future technology leaders.

II. Why are online risks against adolescents?

Based on the above discussion it is pertinent to understand the alarming rise in online crimes against children is intrinsically linked to the pervasive and borderless nature of our connected world and social media. The pictorial representation helps us to understand the probable causes which leads online risks among adolescents. In the following section of this document, we would understand the different forms of online risks against children, adolescents and youths.

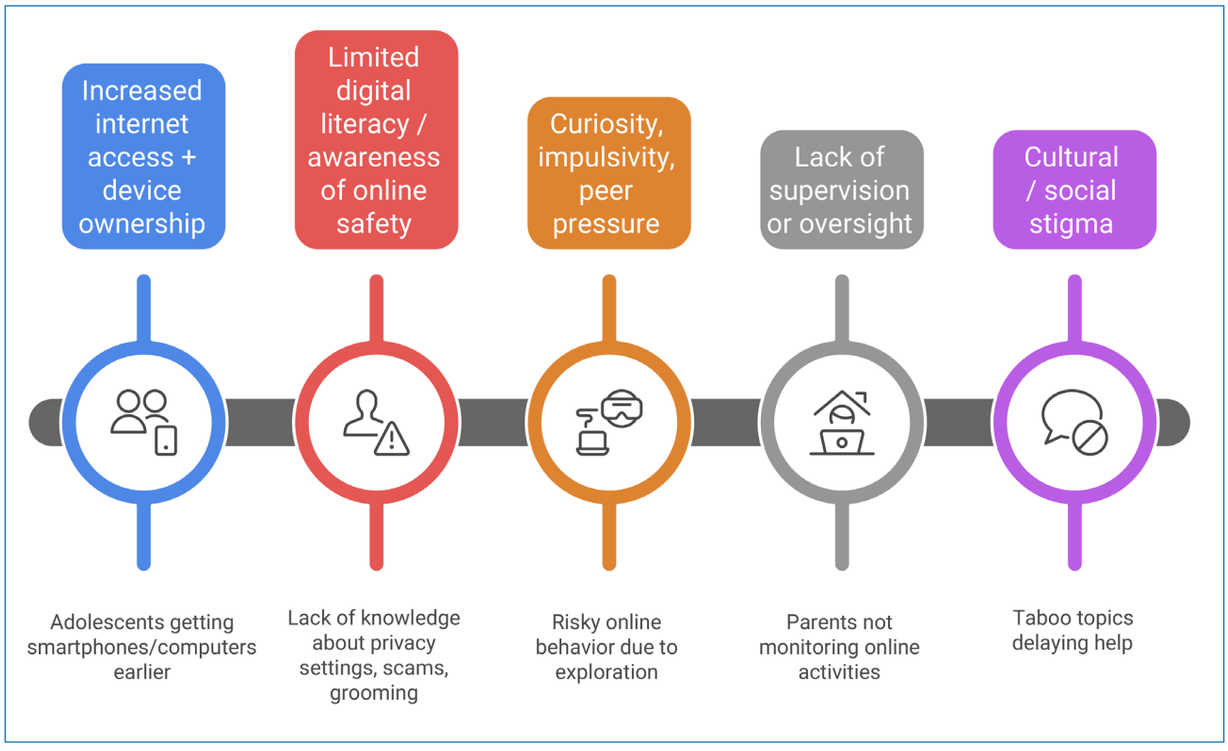


Figure 2: Why online risks with adolescents?

III. Forms of online risks against adolescents

1) Cyberbullying[2]

Imagine being teased or hurt by someone not in person, but through your phone or computer. That's what cyberbullying is: when someone uses the internet, social media, text messages, or other online tools to harm, threaten, or embarrass another person.

2. Cyber Stalking[3]

Cyberstalking is when someone uses the internet or digital tools to repeatedly bother, threaten, or scare another person. It is like a digital version of someone following you everywhere, but using phones, computers, or social media instead of physically being there.

The Hon'ble Delhi High Court (2025), emphasized that online harassment, stalking, and misuse of social media to insult or threaten girls constitute serious criminal offences. The court emphasized that cyberbullying can be as traumatic as physical assault, particularly when directed at children. The anonymity provided by digital platforms often exacerbates the impact on victims. The court called for creating a safe digital environment for children, stating that such protection cannot be restricted to physical spaces alone.

3. Online Grooming[4]

Online grooming is when an adult uses the internet or digital communication to make friends with a child or young person with the secret and harmful goal of abusing or exploiting them. This is very dangerous because children and teenagers may not realize someone is trying to trick them.

4. Non-Consensual Image Sharing (NCIS)[5]

Non-Consensual Image Sharing (NCIS) is the act of sharing or distributing intimate, sexual, or private images or videos of a person without their permission. Children and young people are particularly vulnerable to this form of abuse, and many countries, including India, have legal protections against NCIS.

5. Child Sexual Abuse & Exploitation Material (CSAM)

CSAM is defined as any representation, whether in electronic, print, or any other form, that depicts a child engaged in, or subjected to, real or simulated sexually explicit conduct or activity.

Any act of sexual conduct involving a child is considered abuse under the POCSO Act, the production, possession, transmission, or viewing of material depicting this act is a serious, non-bailable offense, regardless of the artistic merit or context.

[2]IT Act (Sections 66A*, 67), BNS Sections 75, 76, 77, 123.

[3]BNS Section 76 (earlier IPC 354D).

[4]POCSO Act (Sections 11, 12, 13, 14), IT Act Section 67B.

[5]IT Act Sections 67, 67A; BNS Sections 75, 115, 123

6. Sextortion[7]

Sextortion involves a perpetrator obtaining (or claiming to obtain) sexually explicit information or images of the victim, usually through any friendly relationship, account hacking or creating fake content.

7. Phishing and Online Scams

Phishing[8] is a form of online fraud where attackers impersonate legitimate institutions like banks, government agencies, or popular companies to steal personal information.

Online[9] scams might be a fake lottery win, where criminals ask you to pay a "processing fee" to claim your prize, or a romance scam, where someone pretends to be interested in a relationship to get m oney or gifts.

For example, a phishing email might warn you that your bank account has been compromised and urge you to click on a link to "secure your account." This link usually leads to a fake website designed to capture your login credentials or infect your device with malware.

8. Addiction to digital platforms

Addiction to digital platforms, often referred to as digital addiction or internet addiction, is a behavioural condition characterized by an excessive, compulsive need to use digital devices and platforms such as smartphones, social media, online games, and the internet in general[10].

9. Unethical Hacking

It is the unauthorized access to or control over computer systems, networks, or digital data, typically to steal, alter, or destroy information, or to disrupt operations[11].

10. Deepfakes and Impersonation

AI can generate highly realistic fake videos, audio, and images that make it look like a real person said or did something they never did. This is often used for sextortion or defamation.

11. Data Privacy Breach

Every interaction you have with an AI chatbot (the questions you ask, the data you upload) is used to train the model. This means your personal information can become part of the AI's permanent memory.

Online digital risk vulnerability matrix

It is important to understand as why adolescents are particularly exposed to online risks provides a crucial foundation for assessing how these risks manifest in real-world contexts. However, recognizing

[6]IT Act Sections 67B; BNS Sections 316, 352; POCSO Sections 14, 15

[7]IT Act Sections 66E, 67B; BNS Sections 63-73, 95, 96, 294, 295; POCSO Sections 13,14, 15

[8]IT Act Sections 66C (identity theft), 66D (cheating by impersonation)

[9]IT Act Sections 66C, 66D; BNS Section 318 (cheating)

[10]IT Act Sections 67B; BNS Sections 20, 21, 95

[11]IT Act Sections 43, 66

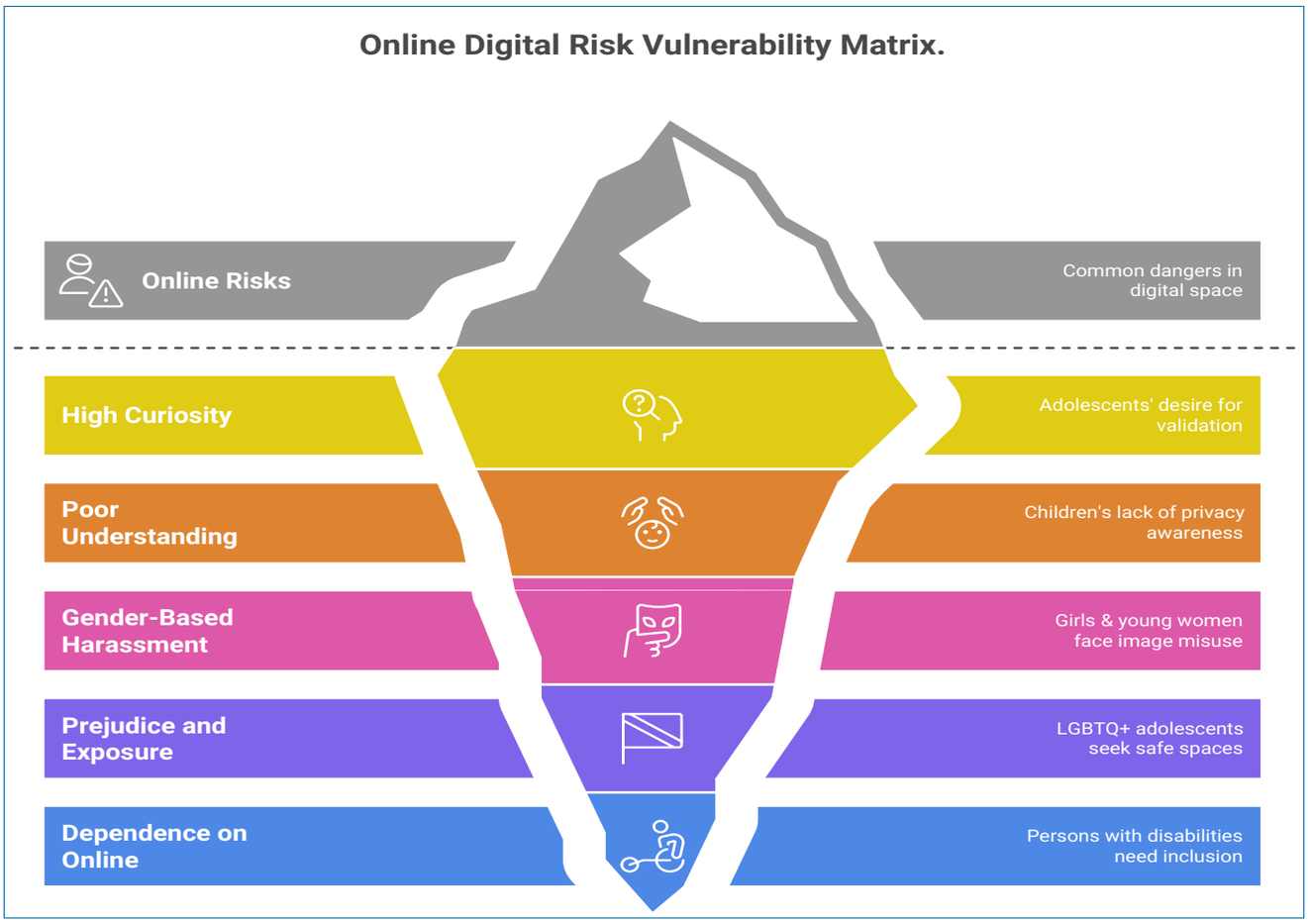


Figure 3: Online Digital Risk Vulnerability Matrix

the causes alone is not sufficient; there is a need to systematically map the varying degrees and types of vulnerabilities they face.

The Online Digital Risk Vulnerability Matrix helps in identifying the group of adolescents which are most at risk of exposure to online harm. There are certain factors such as age, gender, socio-economic background, digital literacy and online behaviour. This matrix not only highlights vulnerability but also emphasizes the need for targeted cyber safety interventions within schools and communities.Together, they highlight the urgent need for adolescents to be equipped with online safety knowledge, enabling them to navigate digital spaces more responsibly and securely.

IV. What is Online Safety?

Think about your personal information—your name, address, phone number, school, or photos. You wouldn't share these loudly in a crowded market, and the same caution applies online. For adolescents, this everyday decision connects directly to the Online Digital Risk Vulnerability Matrix, which helps identify how different types of personal information and online behaviours can increase or reduce exposure to risks. The matrix maps levels of vulnerability—ranging from low to high—based on factors such as what is shared, with whom it is shared, and the platforms being used.

Online or cyber safety, therefore, is not just about avoiding danger but about making informed choices within this matrix of risks. It includes both behavioural practices (like limiting personal information sharing, recognizing unsafe interactions, and communicating respectfully) and technical measures (such as privacy settings, secure passwords, and safe browsing). These actions reduce an adolescent's position in the vulnerability matrix, shifting them from higher-risk to safer zones.

In this framework, stakeholders play a crucial role in influencing an adolescent's placement within the matrix. Positive stakeholders—such as parents, teachers, schools, and regulatory bodies—help lower vulnerability by guiding, educating, and protecting young users. In contrast, negative stakeholders—such as online predators, cyberbullies, or exploitative platforms—can increase risk and push adolescents toward higher vulnerability levels. Understanding this relationship makes online safety a shared responsibility, where awareness, support systems, and informed decision-making work together to help adolescents navigate digital spaces securely and confidently.

Below is a structured classification of positive and negative stakeholders:

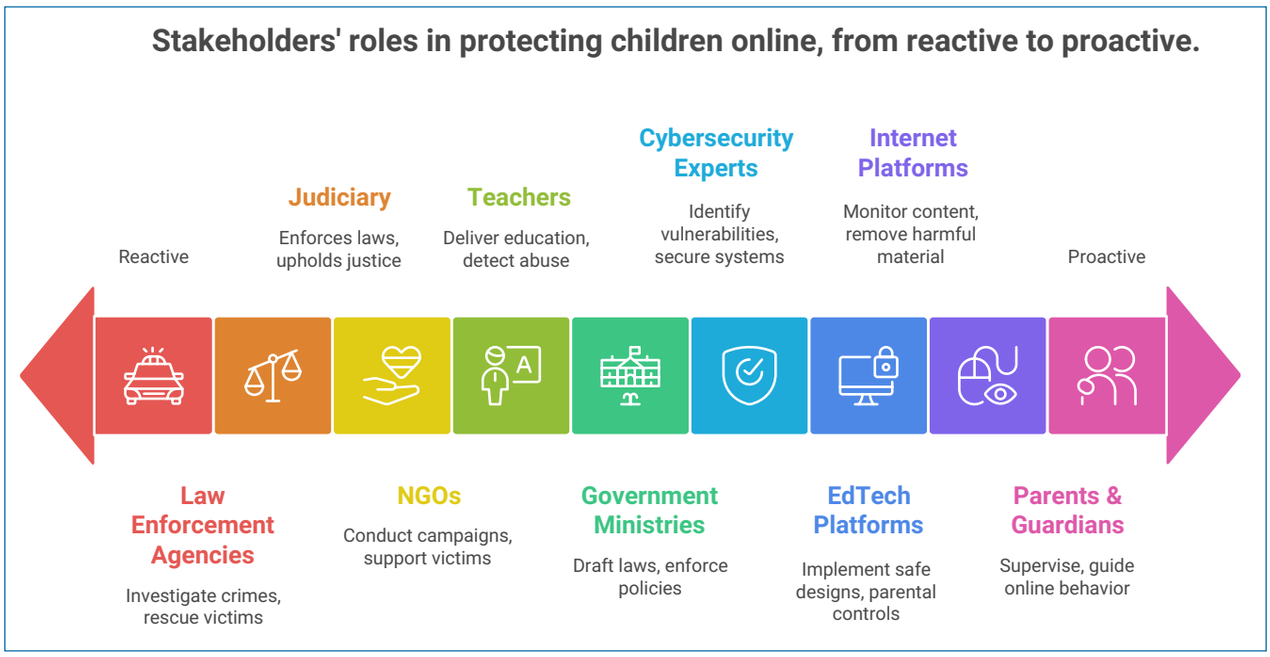


Figure 4: Positive Stakeholders

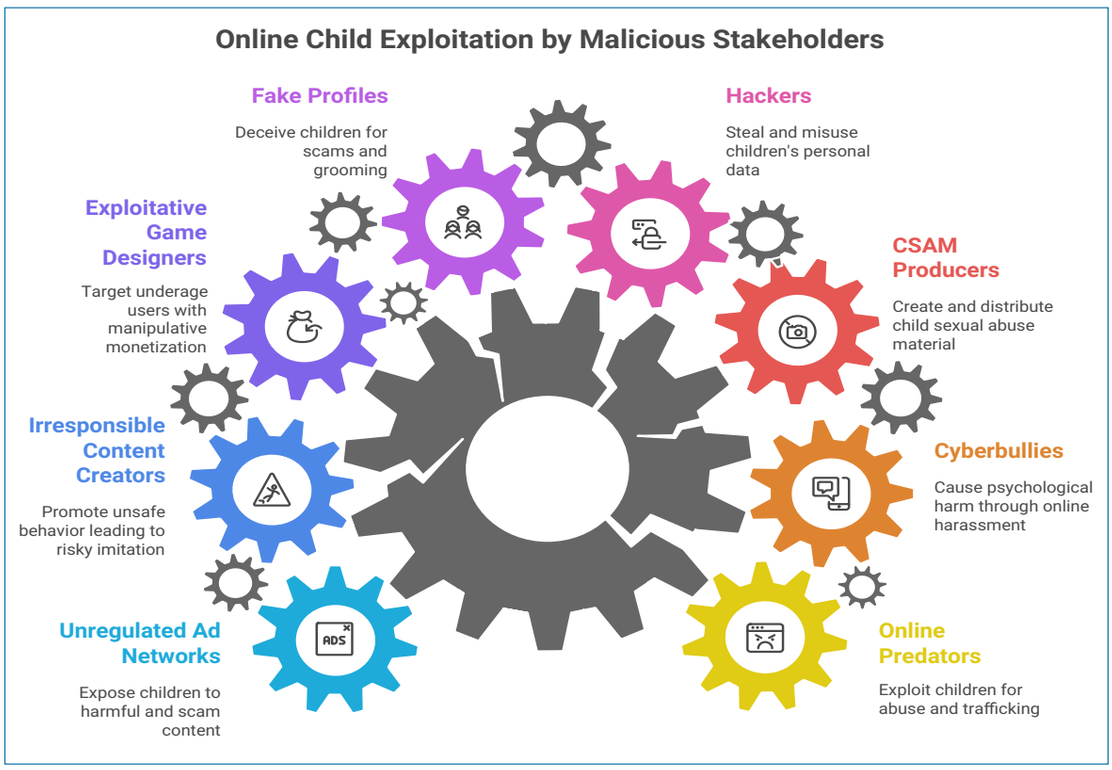


Figure 5: Negative Stakeholders

PART – B
LEGAL & POLICY FRAMEWORK

I. Legal & Policy Framework

Laws protecting adolescents from online risks

Overview of relevant Indian laws and mechanisms related to online safety, including:

Protection of Children from Sexual Offences (POCSO), 2012

Section 11 - 12

- **What it covers:** Defines sexual harassment of a child, including through electronic/digital means (gestures, messages, threats, repeated contact).
- **Punishment:** Up to 3 years imprisonment + fine on first conviction.

Section 13 - 15

- **What it covers:** Use of children for pornographic purposes, storage or possession of child sexual abuse material (CSAM), publishing / distributing pornographic content involving children.
- **Punishment:** More severe punishments; often longer terms, depending on whether offence involves distribution / commercial use etc

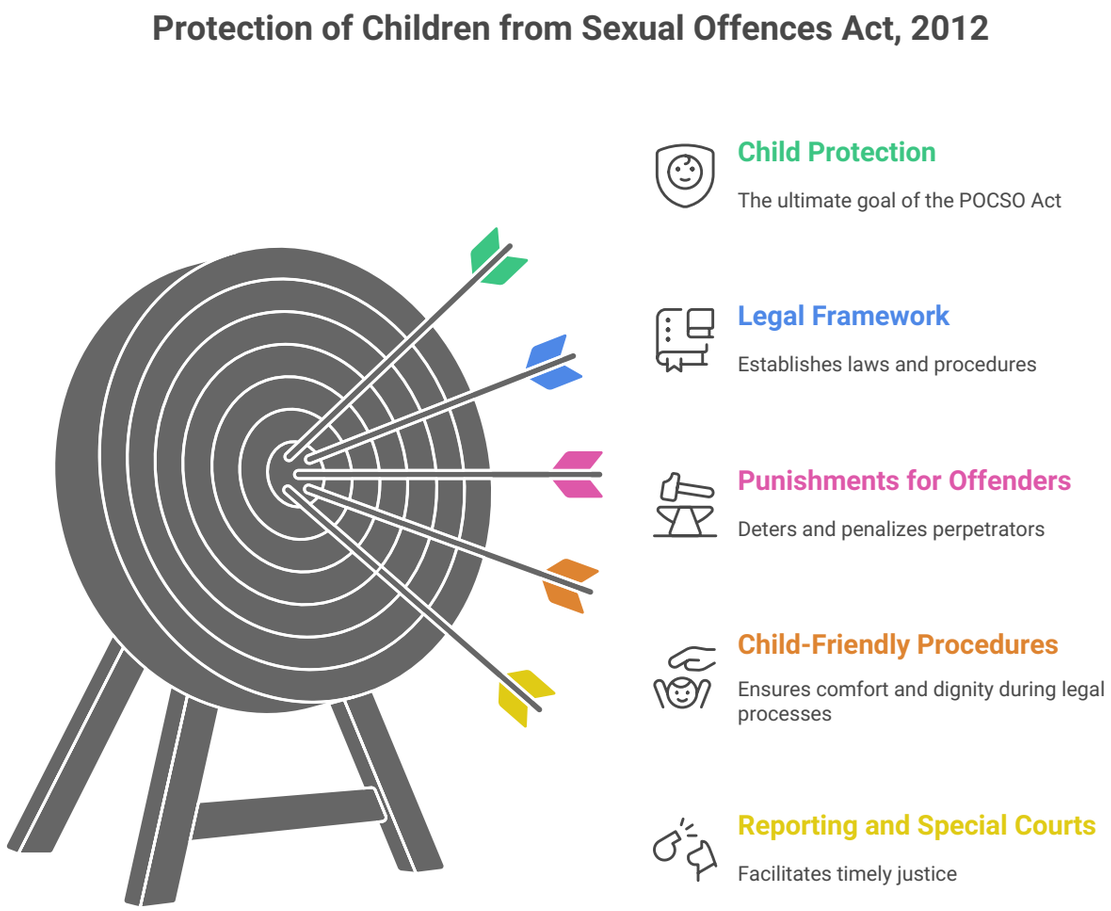


Figure 6: POCSO Act, 2012

Information Technology (IT) Act, 2000

Section 67

- **What it covers:** Publishing/transmitting obscene material online (could affect children if material involves them).
- **Punishment:** Imprisonment up to 3 years and fine up to ₹5 lakh,

Section 67A

- **What it covers:** Publishing/transmitting sexually explicit acts/content electronically; more severe than 67.
- **Punishment:** Imprisonment up to 5 years and fine up to ₹10 lakh.

Section 67B

- **What it covers:** Specifically covering material depicting children in sexually explicit acts, or abusing/ grooming children; includes storing, transmitting, distributing CSAM etc.
- **Punishment:** Imprisonment up to 5 years and fine up to ₹10 lakh.

Information Technology (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021

Obligations for platforms/intermediaries: remove harmful content (including content involving minors), grievance redress, etc. Helps enforce above laws .

Bharatiya Nyaya Sanhita (BNS), 2023

Section 2(3)

- **What it covers:** Defines "child" as person under 18 years; legal basis for all child-related criminal provisions .

Section 78

- **What it covers:** Stalking includes digital/electronic communication / monitoring etc. Useful for cyberstalking / harassment of children (especially female children) .
- **Punishment:** Imprisonment up to 3 years and fine.

Section 79

- **What it covers:** Insulting modesty of any person: via words, gestures, or objects. Now more clearly covers online content / messaging etc .
- **Punishment:** Simple imprisonment for a term which may extend to 3 years, and Fine.

Section 115

- **What it covers:** Sale, distribution or circulation of obscene material. Includes electronic forms. Helpful when obscene content (with or without children) is shared online.
- **Punishment:** Imprisonment which may extend to 1 year OR fine up to ₹10000 or both.

Section 356:

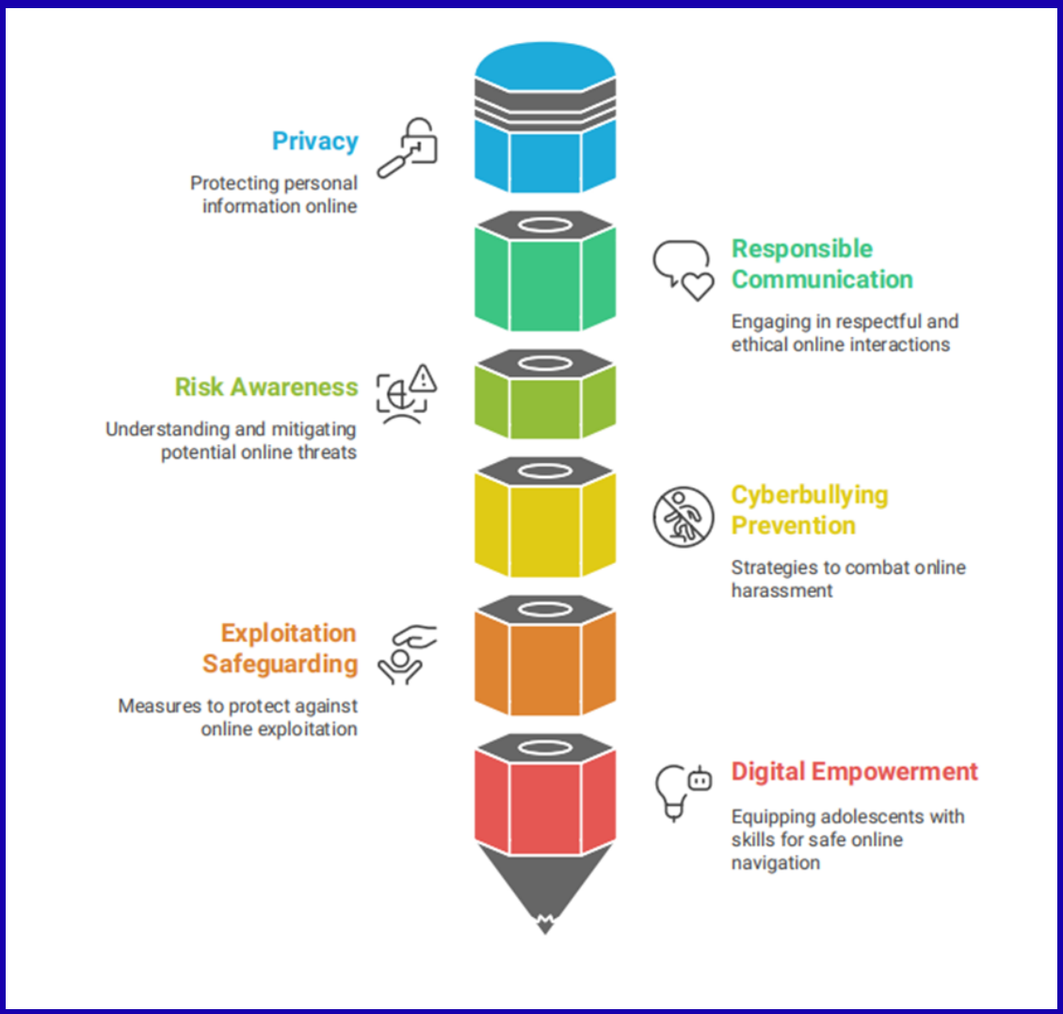
- **What it covers:** Defamation (including online defamation) – making false statements about a child or misleading content that harms reputation.
- **Punishment:** Imprisonment up to 2 years OR fine or both.

Digital Personal Data Protection Act (DPDP), 2023

Section 9

- **What it covers:** Protects children's personal data; requires parental consent, etc.; prevents misuse of children's data which can tie into abuse/exploitation risk .
- **Punishment:** Violation of obligations relating to children's personal data under Section 9 of the DPDP Act, 2023 attracts a penalty up to ₹200 crore under Section 33 read with the Schedule of the Act.

PART – C
GUIDELINES AND STANDARD OPERATING PROCEDURES



I. About the Guidelines & Standard Operating Procedures

Purpose of the Guidelines

These Guidelines aim to promote a safe, responsible, and inclusive digital environment for adolescents in Delhi. They provide a practical framework for preventing online harm, enhancing digital awareness, and establishing safe online behaviour across schools, homes, and communities. The document pairs clear guidelines (behavioural principles and preventive measures) with Standard Operating Procedures (SOPs) (step-by-step responses) for each topic. It is designed as an official policy manual for all Delhi schools to adopt and scale uniformly.

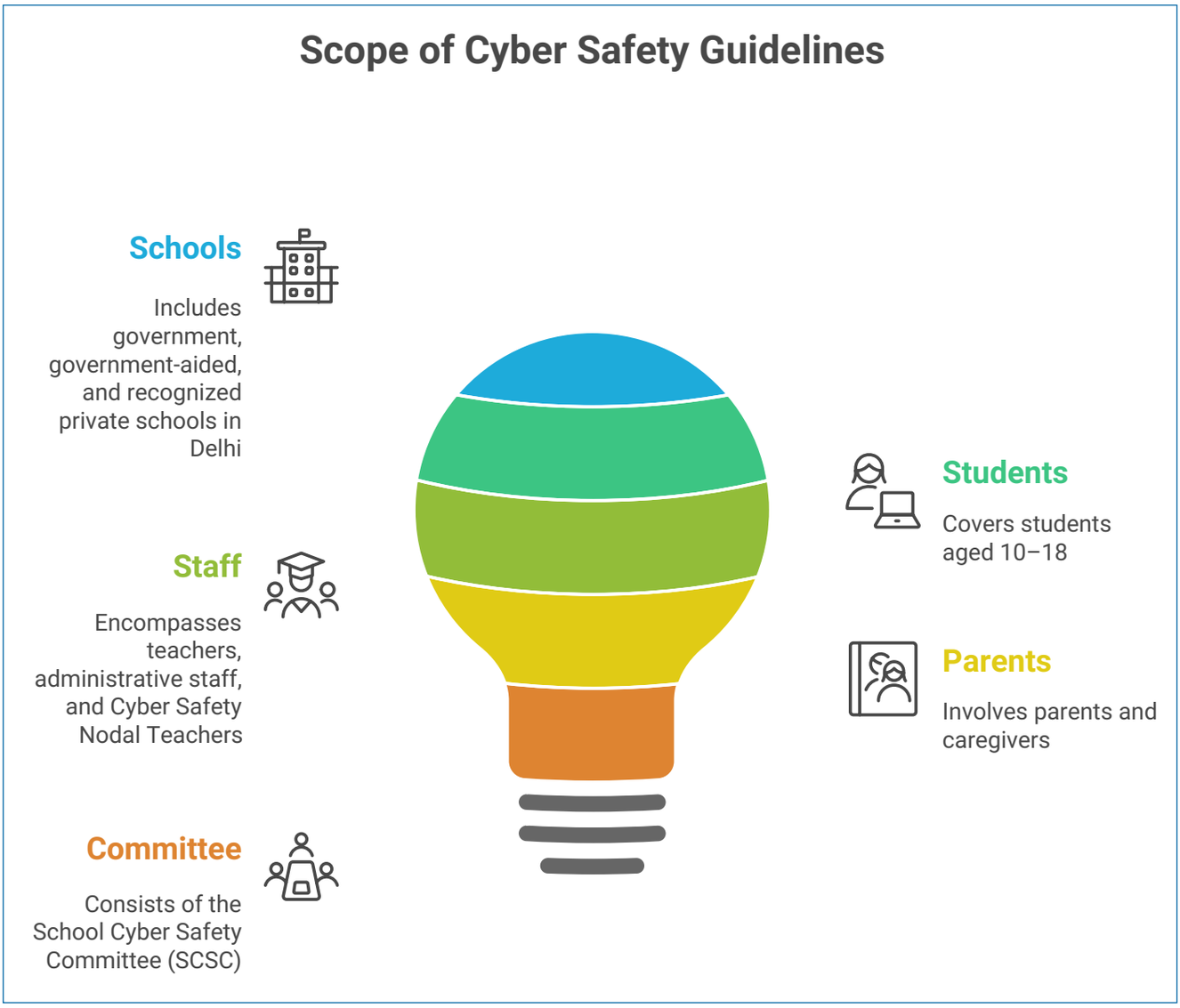


Figure 7: Scope of Cyber Safety Guidelines

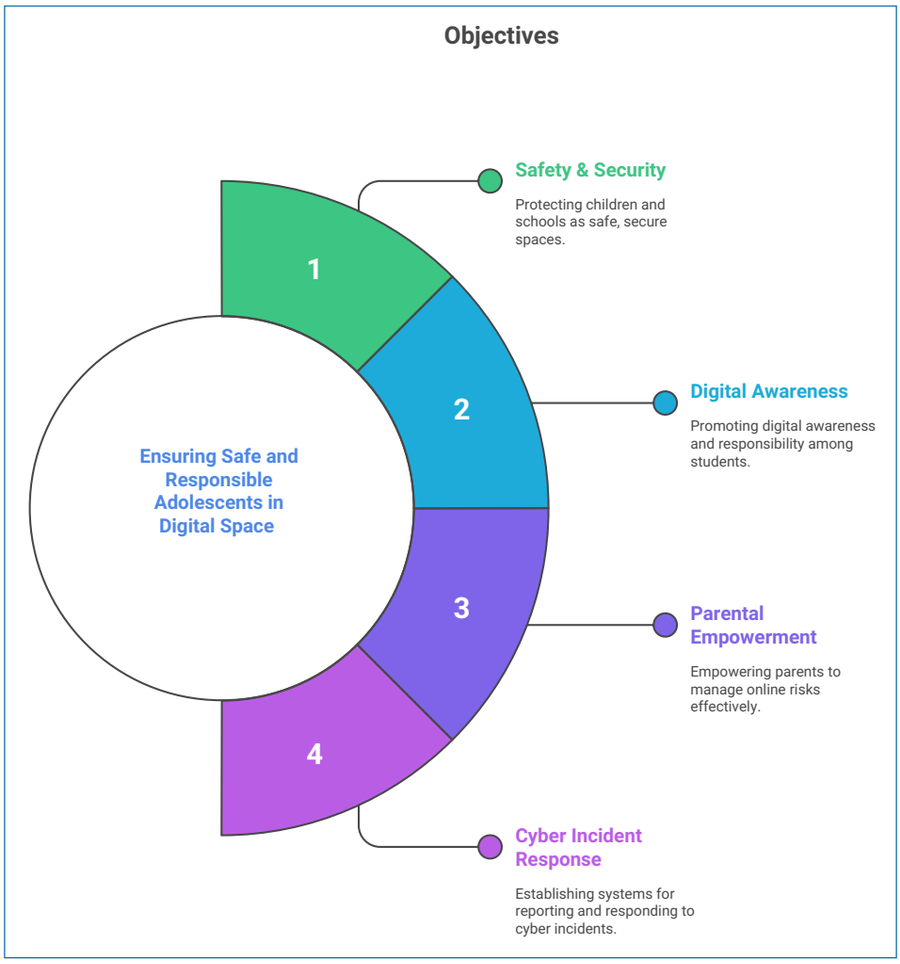


Figure 8: Objectives of Cyber Safety Guidelines

Figure 9: Foundation of Adolescents Online Safety

PART – D
UNDERSTANDING & PREVENTING ONLINE RISKS

I. Cyberbullying

According to NCERT, cyberbullying (harassing via messages, posts, images, exclusion, etc.) harms academic achievement and well-being.

Guidelines:

1. **Empathy:** Teach empathy and respectful communication online; students must never post hurtful or private information about others.
2. **Strong Passwords:** Do not share passwords or let others post using one's account; protect accounts with strong unique passwords.
3. **Privacy:** Understand social media privacy: accept only known friends' request, set strict profiles and location settings, and think before forwarding any message or image.
4. **Encourage bystander intervention:** If a student sees bullying, they should report it rather than join in or stay silent.
5. **Remind students that "The law supports you":** Cyberbullying is a punishable offence under the IT Act and BNS", and victims must tell a trusted adult or call the police (112) if needed.

Response Procedures (SOP):

1. **Immediate Action:** When a cyberbullying complaint or evidence is identified, the teacher or staff member must inform the school cyber safety committee (typically the school principal or counsellor) at once. Record the date, time, and nature of the incident.
2. **Evidence Preservation:** Secure all digital evidence (save chats, screenshots, emails). Do not delete any content. Ensure copies (printed or digital) are available for investigation.
3. **Inform Affected Parties:** Notify the parents/guardians of both victim and alleged bully. Provide counselling to the victim, and notify parents for their guidance. (Support services like school counsellor, psychologist should be offered.)
4. **Investigation:** The School Cyber Safety Committee reviews the evidence. If anonymous or unclear, involve the Cyber Police to trace the source (e.g. device, IP address).
5. **Reporting to Authorities:** If the content is severe (threats of violence, sexual harassment, defamation, or any other similar offense under IT Act), file a report with local police cyber cell or use e-Baalnidan (online cyber helpline). Inform NCPCR or DCPCR if needed. All school staff should be aware that cyberbullying "should be reported".
6. **Follow-up:** Track the student's well-being over time. Update safety filters or classroom rules to prevent recurrence. Document the case in the school's incident log, including actions taken and outcome.
7. **Review & Prevention:** Periodically review policies (e.g. annually) and conduct refresher sessions on cyberbullying to students and staff.

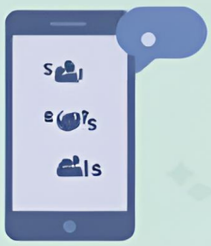
Spot the Signs

Protect Adolescents Online

Adolescent appears anxious, upset, or unusually secretive after using devices.

Sudden withdrawal from offline friends, obsessive phone/computer use, or sleeping badly.

Unexplained unfamiliar accounts/friends or gifts from unknown sources.



Receiving threats, repeated messages, or embarrassing posts about the adolescent.

Stay connected. Watch closely. Keep them safe.

Riya and the Magic Tablet: A Story About Being Safe Online

Once in a colourful neighbourhood in **Delhi**, there lived a curious and creative student named Riya. **Riya** loved drawing, chatting with her friends online, and learning new things on her *Magic Tablet.*

One day, she posted a pretty picture she had drawn in her school group online. At first, her friends said nice things like, *"Wow — you're so talented!" and "I love the colours you used!"*

But then, someone started writing mean messages like:

"Your drawing is silly!"

"Why do you even post this?"

Riya felt her heart sink. The words weren't spoken out loud, but they still hurt. She remembered that her teacher had talked about how some people can sometimes be unkind online, and that this is called **cyberbullying** — when someone uses phones, social apps, or messages to say hurtful things.

Riya didn't feel sure what to do at first, but she did the right thing. She:

- **Stayed calm** (she didn't reply to the mean messages).
- **Saved the messages** so she could show an adult if needed.
- **Blocked** the person who was being unkind.
- **Told her mother and her teacher about it.**

Her teacher smiled and said, "I'm proud of you for speaking up. If someone is unkind online, always talk to a *trusted adult* — like a parent, teacher, or guardian. You're not alone." This is part of being safe online and following good digital habits.

Her mother reminded her of some smart online safety tips — like:

- Not sharing personal details with strangers.
- Using privacy settings so only people she knows can see her posts.
- Talking about anything that makes her uncomfortable on the internet.

With this support, Riya felt brave again. She learned that the internet can be a fun place to *learn* and share, but it also needs to be used wisely and kindly.

II. Online Grooming

Online grooming (when predators befriend children digitally for abuse) is a critical risk.

Guidelines:

1. **Privacy First:** Never share personal details online (full name, address, phone number, school name, passwords) even in chat rooms or with online peers. Students should treat all unknown online contacts as strangers.
2. **Safe Communication:** Discourage one-on-one unsupervised chats. If a stranger or acquaintance requests private conversations or images, stop immediately. Remember that official school online activities should be on monitored platforms (teachers should not use personal accounts).
3. **Education & Awareness:** Teach students the tactics of groomers (e.g. giving gifts, flattery, asking to keep secrets). Run age-appropriate sessions on recognizing cyber grooming and sextortion. Emphasize "parents and teachers should know about your online friends."
4. **Reporting:** Encourage students to tell a parent or teacher immediately if anyone online asks them to meet in person, share intimate photos, or keeps talking about inappropriate topics. No child should feel ashamed to report such contact.
5. **Parental Controls:** Advise parents to enable safe-search filters and child-friendly internet settings at home. Introduce simple tools (e.g. website blockers, restricted accounts).
6. **Teacher-Student Interaction:** As per Delhi child-protection rules, staff must not form personal online relationships with students beyond school tasks. Any question or doubt should involve a parent or counsellor

Response Procedures (SOP):

1. **Immediate Safe Measures:** If grooming is suspected (e.g. child discloses strange online contact), ensure the student's immediate safety. Do not confront the suspect online (to avoid or alerting them).
2. **Preserve Evidence:** Document all communications (messages, screenshots, emails) with dates. Do not delete anything.
3. **Notify:** Inform the child's parents/guardians right away. The parent and school counsellor should be present for any discussion with the child.
4. **Report to Authorities:** As grooming is a serious criminal offense under POCSO and IT Act, report the incident to the police / Child Welfare Committee immediately. Provide all collected evidence. Use child helpline (1098) or cybercrime portal as needed.
5. **Counselling and Support:** Ensure the student receives psychological support from the school counsellor or a child psychologist. Continue to provide a safe and trusting environment at school and at home.
6. **Audit School Networks:** The school IT team should scan and secure any system the student used. Check for malware or keyloggers. Update all filters to block the malicious site or app identified.

Spot the Signs

Protect Adolescents Online

WITHDRAWAL

- Hiding screens online activity, deleting chats.

FEAR & SHAME

- Fear, anxiety, or shame
- Mood swings, anxiety, or irritability.

HIDING

Hiding from family or friends, coping distress which affect, said online interactions.

DEFENSIVENESS

- Sudden defensive reaction when device use is discussed.

Neer and the New Friend Online

Neer was a bright teenager living in Delhi who loved music, games, and chatting with his classmates online. One day, he got a message from someone named *Alex* who said they also loved the same band. At first, the messages were fun — they talked about songs and shared playlists.

After a few chats, Alex started asking more personal questions:

"What school do you go to?"

"Where do you live?"

"Send me photos — I want to see your room."

At first, Neer felt happy to have a new friend. But something didn't feel right. Alex asked him to keep their talks a **secret**, and said things that made Neer uncomfortable. What seemed like a nice chat suddenly made him uneasy. This was an example of online grooming — when someone builds fake trust to get personal information or secrets from you online.

Neer remembered what his teacher and parents taught him about online safety:

- **Don't share personal information like** your school's name, address, photos, or daily routine with people you haven't met in real life.
- **Only talk to real friends you know offline.**
- **Don't keep online chats secret** from adults — secrets that make you nervous are a *red flag*.
- **If someone asks you to do something that feels wrong, stop talking to them, block them, and tell a parent, teacher, or another trusted adult right away.**

Neer did just that. He told his older sister about the messages and showed her the chat. His sister hugged him and said, "You did the smart thing by talking to someone you trust. The internet can be fun, but safety always comes first."

Together, they blocked Alex's account and set stronger privacy settings on Neer's apps so only friends he knew in real life could contact him. Neer also learned that a **real friend never asks for secrets, photos, or private details and never makes you feel unsafe online.**

From that day on, Neer continued to enjoy his online world — listening to music, chatting safely with real friends, and always remembering **to stay cautious, protect his personal details, and speak up if something feels wrong.**

III. Data Privacy Breaches

A privacy breach occurs when personal data (name, ID numbers, photos, etc.) is exposed, stolen, or misused without authorization. This includes hacking of databases, SIM swapping, phishing hacks of email or social accounts, or accidental leaks.

Guidelines:

1. **Personal Data:** Never share personal identifiers (Aadhaar, email passwords, financial information) on public or unknown websites. School-related personal data (reports, photos) should not be posted publicly without permission.
2. **Device and Account Security:** Use strong, unique passwords for all accounts (school portal, email) and change them regularly. Do not share passwords; if a parent must know, it's for safety under supervision. Enable two-factor authentication if available.
3. **Secure Networks:** On school networks, restrict use of USB drives and personal devices that could carry viruses. Only install apps or software that are vetted by the school ICT team.
4. **Data Handling:** Staff handling student records must store data on secured, school-managed systems (password-protected computers or locked cabinets for physical files). When sharing student work online, use school domains or encrypted channels.
5. **CCTV and Biometrics:** If cameras or fingerprint scanners are used at school, inform parents and students about their purpose and data retention. Footage should be stored securely and accessed only by authorized staff for safety.
6. **Compliance:** Follow IT Act provisions for data protection. Appoint a Data Protection Officer if required. Regularly update antivirus and apply security patches on all school devices. Educate students on phishing and spam (e.g. don't click unknown email links).

Response Procedures (SOP):

1. **Immediate Response:** Upon discovery of a data breach (lost device, hacked account, leaked info), immediately secures the system (disconnect from network if needed) and changes compromised passwords.
2. **Assessment:** Determine the scope of breach – what data was exposed and which students were affected.
3. **Notification:** Inform the school administration and affected parties' parents without delay. Follow any legal requirement to notify authorities or data protection regulators.
4. **Remediation:** Remove malware or intruders from the system. Restore data from backups if lost.
5. **Law Enforcement:** If a crime (theft of personal data or hacking) is evident, file a report with cybercrime authorities and provide technical logs.
6. **Documentation:** Record all actions taken in response to the breach. Review and update the school's ICT security policy to prevent future incidents (e.g. stricter access controls, more frequent audits).

Spot the Signs

Protect Adolescents Online

1 UNUSUAL ACTIVITY
Unexpected bank transactions, spam emails, or one-time passwords you didn't request

2 DATA RESALE
Excessive promotional calls or emails after signing up on a new website

3 ACCOUNT BREACHES
Account lockouts or notifications about login attempts from unknown devices

4 NEW LOGIN ALERTS
Google or Apple notifications about new logins or device confirmation emails

PROTECT YOURSELF ONLINE

Monitor accounts regularly • Use strong passwords
Enable two-factor authentication • Stay vigilant

#CyberSecurity #StaySafe #DigitalProtection

Understanding Data Privacy: Aarav's Online Lesson

Aarav was a 14-year-old student studying in a school in Delhi. Like many adolescents, he used the internet every day—for online classes, homework, games, and chatting with friends. His teachers often reminded the class that while the internet is useful, it is important to stay safe online.

One day, Aarav downloaded a new game after seeing an advertisement that promised *free rewards.* The app asked for permission to access his photos, contacts, and location. Without reading carefully, Aarav clicked "Allow."

A few days later, Aarav noticed something strange. His friends told him they were receiving odd messages from his account, and unfamiliar ads appeared on his screen. Aarav felt confused and worried.

That evening, he spoke to his mother, who explained that Aarav might have shared too much personal information without realizing it. She said, "Your **personal data**—like your name, photos, passwords, and contact details—should be protected. When this information is accessed or shared without permission, it is called a **data privacy breach."**

Discussion Question:

What kinds of personal information should be kept private online?

The next day at school, Aarav told his teacher what had happened. His teacher praised him for speaking up and explained that some apps and links collect data in unsafe ways. She reminded the class of important online safety rules:

- Always read permission requests before clicking "Allow"
- Do not share passwords or personal details
- Download apps only from trusted sources
- Tell a trusted adult if something unusual happens online

Aarav now reminds his friends to think before they click and to protect their personal information. By making smart choices online, he learned how to stay safe and responsible in the digital world.

IV. Hacking and unauthorized access

Hacking refers to unauthorized access to or interference with someone's computer systems, accounts, or data. This includes cracking passwords, installing malware, or taking over social media/e-mail accounts.

Guidelines

1. **Secure your online networks:** Set a strong password on Wi-Fi. Keep the router's default admin login changed. Turn off auto-connect to public Wi-Fi. Never to download pirated software/files (they often contain malware).
2. **Regular password update:** Ensure school computers, digital devices at hoem and Wi-Fi are secured (regular password updates). Teach students about phishing and not clicking unknown links in e-mails or messages. Use school firewalls or filters to block malicious sites.
3. **Do not share passwords:** Enable two-factor authentication on social media/email. Log out of shared devices. Be cautious of suspicious e-mails or pop-ups asking for personal info.

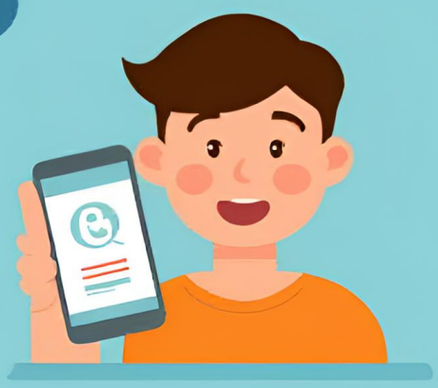
Response Procedures (SOP):

1. **Disconnect device:** Immediately disconnect compromised device from the internet. Change passwords on affected and important accounts from a safe device.
2. **Scan and Clean:** Run antivirus/malware scans to remove any infections. If phone is hacked, notify mobile provider.
3. **Inform Contacts:** If your account was used to spam others, warn your friends/family not to click any links you may have sent.
4. **Report to Authorities:** File a police complaint under Sec. 66 (Hacking, IT Act) and/or relevant BNS sections (cheating, fraud). Use the National Cyber Crime Portal to report identity theft or financial fraud.
5. **Cyber Cell:** Visit a cyber cell or specialized police unit; Delhi has 15 Cyber Crime Police Stations **(Refer Annexure VII).**
6. **Regulatory Bodies:** You can also inform CERT-In (Government's cyber emergency response team) via cert-in.org.in.

Spot the Signs

Keep Your Digital World Safe!

1



Logins from unknown places? That's a red flag!

Privacy in unknown places. This access Denied!

2

Device acting weird? Slow, hot, or crashing?

Lockout might mean someone's in your account, watch out!

3

Locked out suddenly? Someone might be in your account!

Turn on two-factor authentication for extra access protection!

4

Two-factor off? Turn it back on for extra protection!

Two-factor stopped: Subscribe for recovery?

Possibly. Details still:
-- Special cybersecurity tips for families, forgetway (forgot?), consards (concerns?), and alerts.

Using Technology the Right Way: Kabir's Choice

Kabir was a 15-year-old student studying in a school in Delhi. He enjoyed learning about computers and often explored how apps and websites worked. His teachers encouraged students to use technology responsibly and reminded them that skills should always be used for good.

One afternoon, Kabir's friend told him about a trick to guess passwords and enter someone else's online account. "It's easy," his friend said. "No one will know." Kabir felt curious, but also unsure. He remembered learning in class that entering someone's account without permission is called **unauthorized access.**

Discussion Question 1:

Why do you think accessing someone else's account without permission is wrong?

That evening, Kabir thought about it more. He realized that using computer skills to break into accounts, steal information, or change data is known as **unethical** hacking. It can harm people, violate their privacy, and is against the law. Just because something can be done with technology does not mean it *should* be done.

The next day at school, Kabir spoke to his computer teacher. She explained that ethical computer users protect data, respect privacy, and follow rules. She added that **strong passwords, privacy settings, and safe online behaviour** help prevent unauthorized access.

Discussion Question 2:

What problems could happen if someone hacks into another person's account?

Kabir made a responsible decision. Instead of trying the trick, he chose to learn about **ethical hacking**, where computer skills are used legally to improve security and protect systems. His teacher praised him for making the right choice and reminded the class that if they ever feel pressured to do something unsafe online, they should talk to a trusted adult.

Discussion Question 3:

What should you do if someone encourages you to misuse technology?

Kabir learned that being a good digital citizen means using technology honestly, safely, and respectfully. By choosing the right path, he protected himself and others in the online world.

V. Cyberstalking

Cyberstalking is the persistent, unwanted monitoring or harassment of a person via digital means (social media, messaging, email, etc.) that creates fear or distress.

Guidelines

1. **Supervision:** Supervise children's online activity and social contacts. Educate them not to share personal details (full name, school, location, photos) with strangers.
2. **Privacy settings:** Use privacy settings on social media; routinely discuss what apps and sites they use. Set strong passwords and secure home Wi-Fi with strong passwords. Install security updates and antivirus on devices.
3. **Interactions:** Encourage students to report any discomfort from online interactions. Work with parents to monitor cyber incidents or discuss it within School Cyber Safety Committee.
4. **Privacy:** Do not accept friend requests or chats from strangers; verify new online contacts in person. Keep social media accounts private. Limit what you post – once online, information can be saved and shared.
5. **Be SMART:** Follow the SMART principle: Stay Safe (don't share sensitive personal info), Meetup (never meet online acquaintances alone), Accepting Files (don't open unknown attachments), Reliable (verify information sources), and Tell Someone (report anything that troubles you).

Response Procedures (SOP):

- **Immediate Steps:** Block the stalker on all platforms. Do not respond to harassing messages. Save evidence (screenshots, messages, call logs).
- **Parental/Educator Action:** Comfort the adolescent and reassure them it's not their fault. Guide them not to delete messages, as they can serve as evidence.
- **Report to Authorities:** Submit an online complaint at cybercrime.gov.in.Alternatively, go to the cyber and demand an FIR (Section 173 BNSS, 2023). Under Sec 78 of BNS, stalking is an offense.
- **Legal Remedies:** Sec. 66E (privacy), Sec. 67 (obscenity), and Sec. 67A (child sexual content) of IT Act apply to harassing or obscene content.
- **School Action (Educators):** If any school student report cyberstalking, activate the School Safety/Child Protection Committee and follows the procedure as mention in Annexure 1.

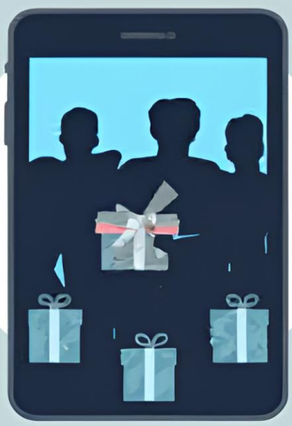
SPOT THE SIGNS

Protect Adolescents Online

1

1. Adolescent appears anxious, upset, or unusually secretive after using devices.

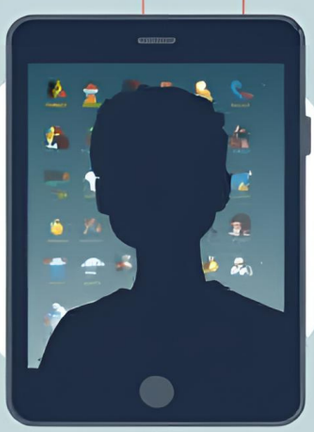
2



2. Sudden withdrawal from offline friends, obsessive phone/computer use, or sleeping badly.

3. Unexplained unfamiliar accounts/friends or gifts from unknown sources.

4



4. Receiving threats, repeated messages, or embarrassing posts about the adolescent.

Staying Safe Online: Meera's Experience

Meera was a 14-year-old student studying in a school in Delhi. She enjoyed using social media to share her drawings and talk with her friends after school. Her teachers often reminded students that the internet can be helpful and fun, but only when used safely and responsibly.

One day, Meera noticed that the same unknown person was liking every photo she posted and commenting on almost everything she shared. At first, Meera ignored it. But soon, the person started sending her repeated messages, even when she did not reply. They asked questions about where she went after school and who her friends were.

Meera began to feel uncomfortable.

This behaviour is called **cyberstalking**. Cyberstalking happens when someone repeatedly contacts, follows, or watches another person online in a way that makes them feel scared, uneasy, or unsafe.

Discussion Question 1:

Why is it important not to respond to repeated or uncomfortable messages?

The next day, Meera's teacher discussed online safety with the class. She explained that cyberstalking can happen to anyone and that students should:

- Keep personal information private
- Accept friend requests only from people they know
- Save evidence of troubling messages
- Report the behaviour to adults, schools, or platforms

Discussion Question 2:

Who are the trusted adults you can talk to if you feel unsafe online?

Meera felt relieved and supported. She learned that being safe online means setting boundaries, trusting your feelings, and asking for help when needed.

By acting wisely, she protected herself and became more confident using the internet.

VI. Non-Consensual Sharing of Images

This refers to distributing or posting another person's private or intimate images/videos without their consent, often to humiliate or blackmail. It is a form of gender-based cyber abuse known as "image-based sexual abuse".

Guidelines:

1. **Personal images:** Discuss the dangers of sharing personal images. Teach students about legal and emotional consequences of sharing images. Encourage respectful online behaviour and clear rules about personal data.
2. **Inform:** Never share photo or video of yourself or others, even privately. If someone pressures you for pictures, decline and report it. Avoid meeting online contacts in private; always discuss with a trusted adult.

Response Procedures (SOP):

1. **Safety First:** If the adolescent is being blackmailed or threatened, instruct them *not to comply*. Preserve evidence (screenshots, chat logs, call records).
2. **Reporting:** File a complaint to cybercrime authorities. Use the National Cyber Crime Portal or NCPCR's POCSO e-Box to report the incident. The e-Box is an online form for reporting sexual offences against children. Include all evidence.
3. **Police FIR:** Visit a police station (women/child cell) and file an FIR. If the victim is a minor, police must register it as a POCSO case (sexual harassment or pornography involving a child). Section 173 of BNSS, 2023 mandates filing of a complaint.
4. **Platform Action:** Report the abusive content to the social media/platform where it appeared (most have "report abuse"). They are required to disable the content quickly. **You can also register a request at StopNCII.org.**

SPOT THE SIGNS

PROTECT ADOLESCENTS ONLINE

Secretive online activity
An adolescent suddenly becomes anxious or secretive about online activity or phone usage.

Deletion of data
Deletion of certain messages or images; closing screens when parents/teachers approach.

Received threatening messages
Being threatened or blackmailed (e.g. "Send me X Rupees or I will leak your photos")

Calls from unknown numbers
Receiving calls/texts from unknown numbers demanding money/images.

Respecting Privacy Online: Ananya's Lesson

Ananya was a 14-year-old student studying in a school in Delhi. She enjoyed chatting with her friends online and sharing photos from school events and family celebrations. Her teachers often reminded students that being online also means respecting others' privacy.

One day, Ananya sent a funny photo of herself to a close friend in a private chat. She trusted that the picture would stay between them. However, a few days later, Ananya discovered that the photo had been shared in a larger group without her permission. Some students were laughing, and Ananya felt embarrassed and upset.

This situation is called **non-consensual sharing of images.** It happens when someone shares another person's photo or video without asking or getting permission first. Even if the image is not harmful, sharing it without consent is wrong and can hurt someone's feelings.

Discussion Question 1:

Why is it important to ask for permission before sharing someone else's photo?

Ananya did not reply to the messages. Instead, she saved screenshots and spoke to her class teacher and parents. They listened carefully and reassured her that she had done the right thing. Her teacher explained that everyone has the **right to privacy**, both offline and online.

Discussion Question 2:

What should Ananya's friend have done before sharing the image?

With support from her family and school, Ananya felt safer. She learned important online safety rules:

- Never share someone's image without permission
- Think carefully before sending personal photos
- Use privacy settings on apps and social media
- Speak to a trusted adult if something online feels wrong

Discussion Question 3:

Who are the trusted adults you can talk to if your privacy is not respected online?

Ananya realized that being a responsible digital citizen means showing kindness, respect, and care for others. By learning from this experience, she and her classmates understood how to use the internet safely and responsibly.

VII. Child Sexual Exploitation and Abuse Material (CSEAM)

NCERT defines such exposure as "circulation, creation and possession of sexually explicit material, especially featuring children".

Guidelines:

1. **Educate:** Educate young adolescents about "stranger danger" online and never to meet strangers or respond to sexual messages. Keep open communication so that children can report uncomfortable online interactions. Be aware of the games/sites they use and join them occasionally.
2. **Refuse & report:** If anyone online (peer or adult) asks a child for sexual photos or tries to get close too quickly, refuse and report it. Never share personal pictures. Block and ignore users who behave inappropriately.

Response Procedures (SOP):

1. **Immediate Safety:** Protect the child first. Remove them from contact if an abusive person is identified. Do not confront the abuser at home – call authorities.
2. **Report to Police and Child Welfare:** Immediately call local police and Childline (1098). Police can register the case under POCSO Act 2012.
3. **Use POCSO E-Box:** Report to the NCPCR's POCSO e-Box, which is designed for directly reporting child sexual offences. This will alert national authorities.
4. **File FIR:** The police (or Juvenile Welfare Officer) should file an FIR. Under POCSO Act, the police must also notify the local Child Welfare Committee (CWC) within 24 hours. CWC will provide protection and can order medical care. (See Anexure VIII)
5. **Evidence Preservation:** Preserve any electronic evidence (messages, photos, call records, screenshots). Do not share them publicly. The police will investigate digital trail.

SPOT THE SIGNS

PROTECT ADOLESCENTS ONLINE

Unexplained Gifts

A child receiving gifts or money from an older person they met online.

Secret Screens

Using devices behind closed doors, switching screens when disturbed.

Late Night Texts

Excessive phone charging, frequent texting late at night, or reluctance to discuss online activities.

Physical Signs

Unexplained bruises or signs of physical abuse.

Staying Safe Online: Rahul Learns to Speak Up

Rahul was a 15-year-old student studying in a school in Delhi. He used the internet every day for schoolwork, watching videos, and chatting with friends. His teachers often reminded the class that the internet is useful, but not everything online is safe or meant for children.

One afternoon, while using a shared computer at home, Rahul accidentally clicked on a link that led to disturbing and inappropriate content involving children. Rahul felt confused and uncomfortable. He quickly closed the page, but he was unsure what to do next.

Material like this is known as **Child Sexual Exploitation and Abuse Material (CSEAM).** It includes images or videos that show children being harmed or exploited. Seeing or sharing such content is never okay, and children are not responsible if they come across it accidentally.

Discussion Question 1:

How do you think Rahul felt when he saw something that made him uncomfortable online?

He immediately told his mother and explained what he had seen. She thanked him for speaking up and reassured him that he had done the right thing.

Rahul's teacher later explained to the class that:

- Children should never search for, watch, save, or share harmful or inappropriate content.
- Accidentally seeing such content is not the child's fault.
- Reporting helps protect other children and keeps the internet safer.

Discussion Question 2:

Why is it important to report harmful content instead of ignoring it?

The teacher also reminded students that if anyone online asks for pictures, videos, or secrets that make them uncomfortable, they should say no, stop communication, and tell a trusted adult immediately.

Rahul felt relieved knowing he was supported.

VIII. Deepfakes (AI-Generated Fake Media)

Deepfakes are realistic synthetic images, audio, or video created using AI (e.g., face-swapping technology) to falsely depict individuals doing or saying things they never did.

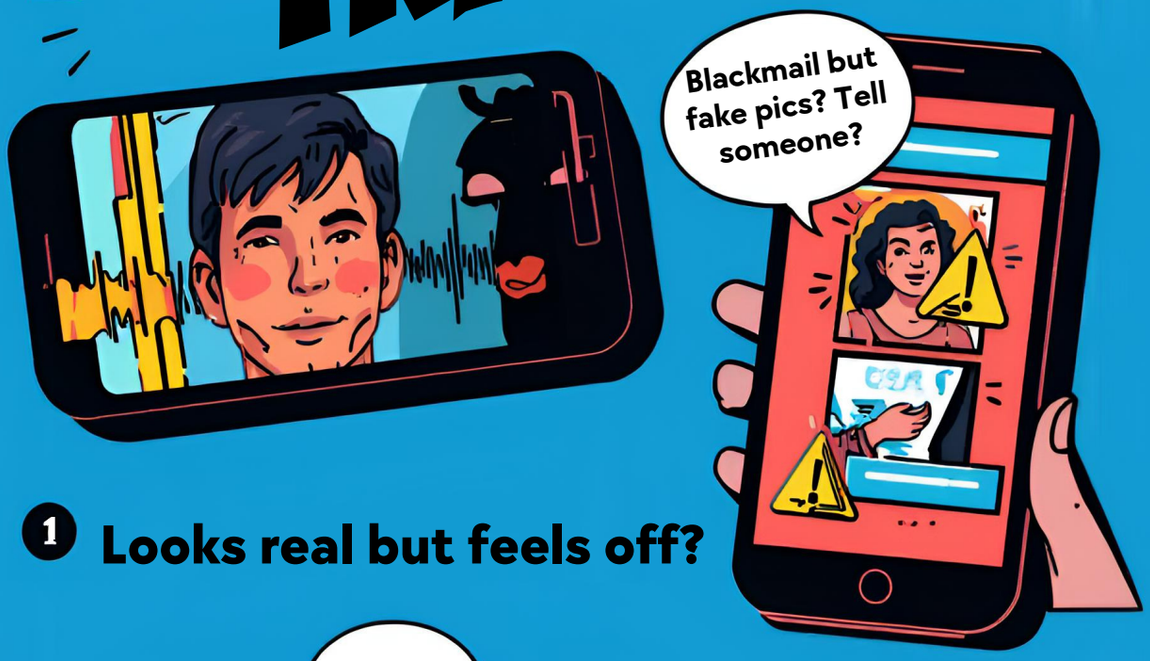
Guidelines:

1. **Critical thinking:** Explain to children that not everything seen online is real. Encourage critical thinking: verify news and videos from reputable sources before believing or sharing. Keep family photos and videos private to prevent misuse.
2. **Media literacy:** Teach digital literacy: how to spot manipulated media (e.g., odd lighting, face movement). Warn students about copying or spreading videos without verification.
3. **Be cautious:** Be cautious if you find videos of yourself online – ask trusted adults for help if you suspect it's a deepfake. If encountering a suspicious video, check if multiple trustworthy sources report it.

Response Procedures (SOP):

1. **Verify Before Acting:** If you see a suspicious media clip involving you or someone you know, consult experts or use online deepfake detectors.
2. **Report Content:** If a deepfake of a child/teen is being circulated (especially sexual in nature), report it to the platform immediately (social media sites have abuse-report tools). As per the 2021 IT Rules, platforms must take down illegal content quickly.
3. **Legal Action:** File a police complaint treating the deepfake as defamation or privacy breach. The victim's guardians can also issue legal notices. Courts have granted injunctions against deepfakes (cease-and-desist).
4. **Government Mechanisms:** Use the National Cyber Crime Portal if the content is harmful or criminal nature. Although no special deepfake law exists, MeitY has advised platforms to remove deepfakes within 3 hours of notice.
5. **Support:** For reputation protection, you may discuss it with lawyer, if needed.

WATCH OUT FOR DEEPFAKE TRICKS!



1 **Looks real but feels off?**

Blackmail with fake pics?

Someone's face or voice weirdly?

Seeing Isn't Always Believing: Ayaan and the Fake Video

Ayaan was a 14-year-old student studying in a school in Delhi. He enjoyed watching short videos online and sharing interesting clips with his friends. His teachers often reminded students that not everything seen on the internet is real and that it is important to think carefully before believing or sharing online content.

One evening, Ayaan received a video in a class group chat. The video showed a well-known school student saying and doing strange things. Many students were shocked and started forwarding the video quickly. Ayaan felt confused because the student in the video did not behave like that in real life.

This kind of video is called a deepfake. A **deepfake** is created using technology that can change or replace a person's face, voice, or actions to make something look real when it is not.

Discussion Question 1:

Why do you think people might believe a deepfake video easily?

Ayaan decided not to forward the video. Instead, he showed it to his older sister, who explained that deepfakes can be used to spread false information, embarrass people, or harm their reputation. Sharing such content can hurt others and create problems, even if it is done as a joke.

The next day at school, Ayaan's teacher discussed online safety with the class. She explained that students should:

- Think before believing or sharing videos and images
- Check information from trusted sources
- Never forward content that could hurt or shame someone
- Report suspicious or harmful content to a trusted adult

Discussion Question 2:

What should you do if you receive a video or image that seems fake or makes you uncomfortable?

Ayaan learned an important lesson: just because something looks real online does not mean it is true. Staying safe online means thinking carefully, respecting others, and asking for help when unsure.

IX. Addiction to Gaming Platforms

The WHO defines gaming addiction as a pattern of gaming behaviour marked by loss of control and prioritizing games over other activities, despite negative consequences. In India, health authorities acknowledge that unrestricted gaming can lead to serious mental health issue.

Guidelines:

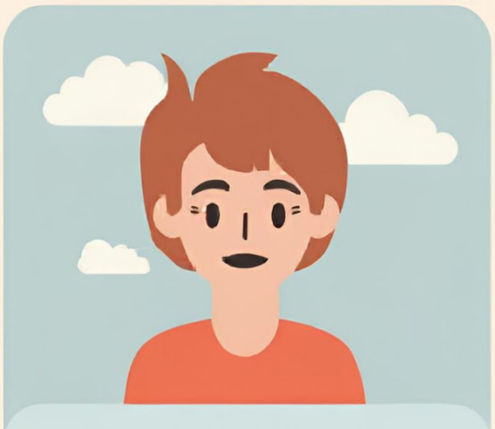
1. **Establish clear rules:** Inform parents to set daily screen-time limits and enforce device curfews (e.g., no games during homework time or after 9 PM). Encourage offline hobbies and physical activities.
2. **Talk:** Talk about the risks of gaming too much (poor sleep, eyestrain, isolation) and set a healthy example with your own screen use.
3. **Educate:** Encourage physical activities in schools. Educate students about responsible digital use.
4. **Practice self-control:** Encourage students to take regular breaks, keep track of playing time (use phone alarms or apps). Participate in social or sports activities outside gaming. Seek help if they feel anxious without game, or use gaming to cope with problems.

Response Procedures (SOP):

1. **Dialogue:** Parents/educators should address the issue calmly. Acknowledge the child's interest but explain concerns. Together, set stricter time limits and use software timers.
2. **Professional Help:** If addiction is severe, consult a paediatrician or mental health professional (psychiatrist/psychologist) for counselling.
3. **Positive Alternatives:** Gradually replace gaming time with rewarding activities (sports, arts, spending time with family/friends) to fill the void. Encourage joining clubs or classes.
4. **Monitor and Adjust:** Keep devices in common areas and restrict gaming accounts.
5. **Leverage Government Advice:** Follow the Ministry of Education's advisories on healthy gaming habits and discuss them with the child. Schools may circulate these advisories to parents.

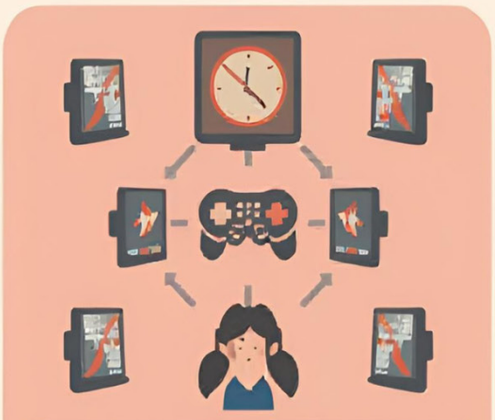
Spot the Signs

Protect Adolescents Online



- Mood swings, aggression or anxiety when not gaming

- Missing homework, meals, or sleep



- Playing for many hours without breaks

- Eye strain, headaches, neck or wrist pain.

Finding Balance Online: Arjun and the Game Clock

Arjun was a 14-year-old student studying in a school in Delhi. He enjoyed playing online games after finishing his homework. Gaming helped him relax and connect with his friends. His teachers often reminded students that technology can be fun and useful when used in a balanced way.

Over time, Arjun started spending more and more hours playing games. He stayed up late to finish levels and felt upset when he could not play. He stopped going out to play cricket and found it hard to concentrate in class. Even during meals, he kept thinking about the game.

This kind of behaviour can be a sign of **gaming addiction**, which happens when gaming starts to take over daily life and affects sleep, studies, health, or relationships.

Discussion Question 1:

How can playing games too much affect a student's daily life?

One day, Arjun's teacher noticed that he looked tired and distracted. She gently spoke to him and encouraged him to talk about his routine. Arjun realised that gaming had become more important to him than schoolwork, rest, and spending time with family.

At home, Arjun shared his feelings with his parents. They listened carefully and explained that gaming itself is not bad, but too much of anything can be harmful. Together, they made a simple plan: fixed screen time, regular breaks, outdoor activities, and no gaming before bedtime.

Discussion Question 2:

Why is it important to have limits on screen time and gaming?

With these changes, Arjun slowly felt better. He slept well, focused more in class, and enjoyed playing sports again. He still played games—but only for a limited time and after completing his responsibilities.

Discussion Question 3:

What can you do if you feel gaming is taking up too much of your time?

Arjun learned that being safe online also means taking care of your body and mind. By finding balance and asking for help, he became a healthier and more responsible digital user.

X. Digital Payments Scam

A digital payment scam happens when someone tricks you online or on the phone into sending money or sharing your OTP or UPI PIN.

Guidelines:

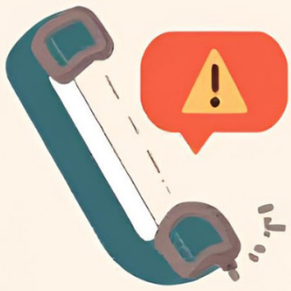
1. **Never Share Your UPI PIN or CVV.** These are like the keys to your bank vault. No bank or payment app will ever ask you for your PIN, CVV, or full card number, even if they claim there is a "problem" with your account.
2. **OTP Security:** Treat the OTP (One-Time Password) as a Secret Code. An OTP is only used for receiving money or authorizing a transfer. If someone asks you for an OTP to receive a prize or refund, it is always a scam.
3. **App Downloads:** Use Official Apps Only. Only download payment apps (like banking apps, UPI, or wallets) from the official Google Play Store or Apple App Store.
4. **Scanning Codes:** Always Check the QR Code Details. Before scanning a QR code to pay, always verify the name of the person or business that pops up on your screen. Criminals can place fake QR codes in public places (like bus stops or shops) to divert your payment to their account.

Response Procedures (SOP):

1. **Do NOT share OTPs** or respond further to the fraudster.
2. **Freeze account:** By turning on "Secure/Deactivate UPI" in app and deactivate debit card via bank app.
3. **Take a screenshot of :** transaction history, fraudulent message/QR code and phone number/ profile involved.
4. **File a complaint:** at https://cybercrime.gov.in or Call 1930 – National Cybercrime Helpline for immediate blocking/recovery support.

Spot The Scam Signs!

Protect Adolescents Online



Persistent Payment Demands

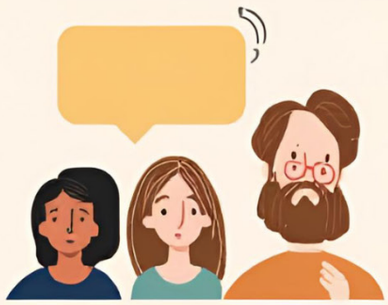
Repeated calls/messages demanding immediate payment.

Unknown Links & QR Codes

Receiving unknown links, Apps, or QR Codes.

Fake Authority Figures

Pretending to be bank staff, customer care, police, school, or friends.



Suspicious Messages

Messages with spelling errors or unusual tone.

Paying Smart Online: Neha Learns a Safety Lesson

Neha was a 15-year-old student studying in a school in Delhi. She often used her parents' phone to recharge mobile data, book tickets, and pay for small items using digital payment apps. Her teachers had explained that while digital payments are fast and convenient, they must be used carefully.

One afternoon, Neha received a message that looked like it came from a well-known payment app. It said, *"Your account will be blocked today. Click here to update your details."* The message also asked for her one-time password (OTP).

Neha felt worried. She did not want the account to stop working. Just as she was about to click the link, she remembered her school's online safety lesson. She knew that real banks and payment apps never ask for passwords or OTPs through messages or calls.

This type of trick is called a **digital payment scam.** Scammers try to scare or rush people into sharing private information so they can steal money.

Discussion Question 1:

Why do scammers try to create fear or urgency in such messages?

Instead of responding, Neha showed the message to her father. He praised her for being alert and explained that clicking unknown links or sharing OTPs can lead to loss of money. Together, they reported the message and deleted it.

The next day, Neha's teacher discussed digital safety in class. She reminded students to:

- Never share OTPs, PINs, or passwords
- Check messages carefully for spelling mistakes or strange links
- Use digital payments only under adult guidance
- Report suspicious messages immediately

Discussion Question 2:

Who should you talk to if you receive a suspicious payment message or call?

Neha now understands that digital payments are helpful tools—but only when used wisely and safely. By staying alert and informed, she helps protect herself and her family from online scams.

XI. In-App Purchases

Many popular online games are free to download but encourage you to spend real money on in-game items (skins, coins, passes). This can lead to serious financial problems if not managed correctly.

Guidelines:

1. **"Free" Gold/Coins Scams:** Be cautious of websites or messages promising free in-game currency (Gold, V-Bucks, Gems) if you log in with your game account details. These are usually attempts to hack your gaming account and steal any linked payment information.
2. **Loot Box Addiction:** Understand the psychology behind "loot boxes" or "mystery bundles." These are designed to be addictive, often encouraging endless spending for the slim chance of getting a rare item.
3. **Account Selling/Buying:** Do not attempt to buy or sell gaming accounts outside of the official platform. You will almost certainly be scammed, losing both the money you paid and your original account.

Response Procedures (SOP):

1. **Report:** within the game/app using "Report User," "Abuse," "Cheating," or "Harassment."
2. **Inform:** parents/guardians immediately.
3. **If the incident involves sexual content, extortion, or threats:**

- Report at cybercrime.gov.in (Report Women/Child Related Crimes)
- Call 1098 (Childline) for child protection support

4. School should record the case under the School Child Protection Committee.

M-Kavach 2 is a comprehensive mobile device security solution addressing emerging threats related to Android-based mobile devices. The major emphasis is on advising the users against Security misconfigurations, Detection of hidden & sideloaded apps, and scanning the device for risky apps installed on the user's mobile device.

Spot the Signs

Protect Adolescents Online

Declining grades or skipping school, chores, or social activities to play games.

Preoccupation with gaming (talking about games constantly, planning next session).

Loss of sleep due to late-night gaming; poor personal hygiene.

Headaches, fatigue etc.

Watch for these in-app purchase warning signs.
For support and more info, talk to your school counselor or your parent.

Spending Wisely Online: Kunal's Game Lesson

Kunal was a 13-year-old student studying in a school in Delhi. He enjoyed playing games on his tablet after finishing his homework. Many of the games were free to download, which made them fun and easy to start playing.

One day, while playing his favourite game, a message appeared on the screen:

"Buy gems to unlock the next level!"

The game showed bright pictures and a timer that said, "Offer ends soon!"

Without thinking much, Kunal clicked the button. The game used the payment details already saved on the device. Later that evening, Kunal's father noticed an unexpected charge on his phone bill. Kunal felt surprised and worried.

This happened because of an in-app purchase. **In-app purchases** are payments made inside an app or game to buy extra features, levels, or items. Sometimes, apps encourage users to spend money quickly without fully explaining the cost.

Discussion Question 1:

What steps could Kunal have taken before clicking the purchase button?

The next day at school, Kunal's teacher discussed online spending safety. She reminded students to:

- Always ask an adult before making online purchases
- Read pop-ups carefully before clicking
- Understand that "free" apps may still cost money
- Set spending limits and use parental controls

With these lessons, Kunal became more careful while gaming. He learned to enjoy games for fun, not just for rewards. He also understood that being safe online includes being smart about money.

Discussion Question 2:

How can talking to parents or teachers help prevent online spending problems?

Kunal learned that responsible digital behaviour means thinking before clicking, respecting money, and asking for help when unsure.

XII. Call Bombing

Call Bombing (also called call flooding or OTP bombing) is a form of cyber harassment where a person intentionally makes hundreds of missed or voice calls, or triggers repeated OTP/verification calls, to disturb, scare, embarrass, or harass someone.

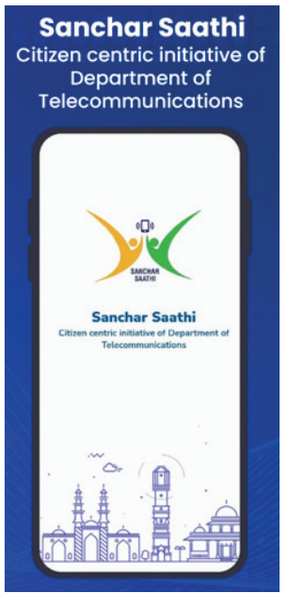
Guidelines:

1. **Stay calm** and do not panic.
2. **Do not answer or engage** with unknown or repeated callers.
3. **Block the number(s)** and activate spam-call or "silence unknown callers" features on your phone.
4. **Save evidence** by keeping call logs, screenshots, dates, and timings.
5. **Inform a trusted adult**—parent, guardian, or teacher—immediately.

Response Procedures (SOP):

1. **Ensure Personal Safety and Stay Calm:** Do not panic or feel scared. Remember that repeated unwanted calls are not your fault.
2. **Do Not Engage with the Caller:** Do not reply to messages asking you to "pick up" or respond.
3. **Use Phone Safety Controls:** If calls continue from multiple numbers, switch to Do Not Disturb temporarily.
4. **Inform a Trusted Adult Immediately:** Tell your parent, guardian, teacher, school counsellor, or school authority.
5. **Report the Incident (With Adult Support):** Call the National Cyber Crime Helpline – 1930 or report online at www.cybercrime.gov.in.

Sanchar Saathi is a citizen centric initiative of Department of Telecommunications (DoT) to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives. **Download the sancchar saathi app from google playstore/apple playstore**



Spot the Signs

Protect Adolescents Online

The adolescent appears anxious, scared on ringing phone.

Fear of phone use or answer calls.

Confusion about 'what went wrong,' or 'what they clicked'.

Threats like "police action" or 'account suspension'.

Staying Calm and Safe: Ishaan and the Endless Calls

Ishaan was a 14-year-old student studying in a school in Delhi. He used his mobile phone to talk to friends, attend online classes, and stay in touch with his family. His teachers often reminded students that phones should be used responsibly and safely.

One evening, Ishaan's phone started ringing again and again. The calls came from unknown numbers, one after another, without stopping. When he answered one call, there was no one speaking on the other side. Soon, his phone battery began to drain, and Ishaan felt anxious and disturbed.

This kind of behaviour is called **call-bombing**. Call-bombing happens when someone makes many repeated calls or uses apps or websites to flood a person's phone with calls, messages, or alerts. It is done to trouble, scare, or harass someone.

Discussion Question 1:

How do you think repeated calls like this can affect a person's feelings and daily life?

The next day, Ishaan told his class teacher about the incident. She explained that call-bombing is a form of **online harassment**

- Never share your phone numbers online
- Avoid responding to repeated unknown calls
- Use blocking and reporting features
- Inform a trusted adult immediately

Discussion Question 2:

What steps did Ishaan take to handle the situation safely?

With help from adults, the calls stopped. Ishaan felt relieved and confident again. He also learned to be more careful about where he shared his phone number online.

Ishaan understood that staying safe online also means protecting your phone and personal details. By staying calm and asking for help, he handled the situation wisely and learned how to use mobile phone more responsibly.

PART – E
DEVICE RELATED RISKS

I. Phishing

Phishing is when someone pretends to be a bank, school, game, or friend to trick you into sharing your password, OTP, or personal details. It can cause loss of money and harm, so never share such information online.

Guidelines:

1. **Verify messages** claiming urgency, prizes, or threats. Do not click unknown links or download attachments from emails/messages.
2. Follow the **STOP–CHECK–CONFIRM–TELL** rule before responding online.
3. **Never share** OTPs, passwords, UPI PINs, or Aadhaar details to any unknown person.

Response Procedures (SOP):

1. **Report to your parents:** With the help of your parents secure your accounts and contact banks immediately on their customer care number.
2. **Disconnect from the internet:** Switch-off the internet immediately if you have already shared your details.
3. **Report to Authorities:** Call at national Cyber Crime Helpline: 1930 or Online complaint: cybercrime.gov.in.

Signs to Watch For:

1. Messages creating panic ("Account blocked today", "Urgent verification")
2. Requests for OTPs, PINs, or passwords.
3. Fake websites mimicking banks or apps.
4. Unexpected prize, refund, or job offers.
5. Unauthorized transactions or login alerts.

Story: The Free Game Coins Message

Ravi loved playing online games after school. One day, he got a message on his phone saying,

"Congratulations! You have won free game coins. Click the link and enter your game password to collect them."

Ravi felt excited and was about to click the link. Just then, he remembered what his teacher had said in class:

"Never share your password or OTP with anyone online."

Ravi showed the message to his mother instead. She checked it and told him it was **fake**. The message was trying to **trick** him into sharing his password. Ravi blocked the sender and reported the message.

Because Ravi **stopped, checked, and told a trusted adult**, his game account stayed safe.

Classroom Message

If a message promises prizes or asks for passwords or OTPs, it is likely phishing. Stop, don't click, and tell a trusted adult.

II. Stalkware

Stalkware is a secret app that someone puts on a phone or computer to spy on another person.

Guidelines:

1. **Avoid phone access:** Do not allow unknown persons to access the child's phone.
2. **Be Alert:** If somone tries to control your device or forces you to install an application i.e. app do not agree and report it immediately to a trusted adult or authority

Response Procedures (SOP):

1. **Immediate Steps:** Stop using the device for sensitive communication. Do not uninstall apps until advised (evidence may be lost).
2. **Reset device** and change all passwords.
3. **Report to Authorities:** Call at national Cyber Crime Helpline: 1930 or Online complaint: at **cybercrime.gov.in.**

Signs to Watch For

1. Device overheating or battery draining fast.
2. Phone behaving abnormally or apps opening automatically.
3. Unknown apps with admin or accessibility permissions.
4. Someone knowing private conversations.

The Phone That Knew Too Much

Riya was a 14-year-old student who lived in a busy neighbourhood and loved using her phone to talk to friends, listen to music, and do schoolwork. Her phone felt like her personal space—a place where she could be herself.

One day, Riya noticed something strange. Her phone battery was draining very fast, even when she was not using it. Some apps opened by themselves, and her phone felt slow. What surprised her most was that someone seemed to know where she had been and who she talked to.

Riya felt confused and uncomfortable.

She decided to tell her older cousin, Aman, who knew a lot about technology. Aman checked her phone and explained, "Riya, there may be a hidden app on your phone called stalkware."

Stalkware is software that secretly watches what someone does on their phone. It can track messages, calls, photos, and even location—without the person knowing or agreeing.

Riya felt worried. "That doesn't feel right," she said.

Aman nodded. "You're right. Stalkware is wrong because everyone has the right to privacy."

Together, they told Riya's parents and a teacher at school. With help from trusted adults, the unsafe app was removed, and Riya learned how to protect her phone using strong passwords and safe settings.

Riya felt relieved. She also learned something important: if a device behaves strangely or makes you feel watched, it's okay to speak up and ask for help.

Classroom Message

If your device behaves strangely, tell a trusted adult. Asking for help is a smart and brave choice.

III. Ransomware

Ransomware is a bad computer virus that locks your files or device and asks for money to unlock them. It can come from fake games, free downloads, or unsafe links, so always be careful about what you click or install.

Guidelines:

1. Prohibit downloading pirated software or games. Ensure school devices have licensed security software.
2. Do not download free versions of paid games/apps.
3. Avoid clicking pop-ups or "urgent update" links.

Response Procedures (SOP):

3. Disconnect device from internet immediately.
4. Do not pay ransom.
5. Preserve ransom message as evidence.
6. Seek technical support for data recovery.
7. **Report to Authorities:** Call at national Cyber Crime Helpline: 1930 or Online complaint: at cybercrime.gov.in or to the nearest cyber police station.

Signs to Watch For

1. Files suddenly locked or renamed
2. Ransom message demanding payment
3. Inability to access documents or apps
4. System crashes or extreme slowdown

Story: The Locked Computer

Arjun downloaded a free game from a website he did not know. At first, the game looked fine.

The next day, when Arjun switched on his computer, all his files were locked. A message popped up saying,

"Pay money to unlock your computer."

Arjun felt scared and called his father. His father told him not to pay and disconnected the computer from the internet. With help from a computer expert, the virus was removed.

Arjun learned an important lesson: free downloads from unknown websites can be dangerous.

Classroom Message

Only download games and apps from trusted places, and never click unknown links.

IV. Malware Attack

Malware refers to harmful software such as viruses, worms, trojans, or spyware designed to damage devices, steal data, spy on users, or disrupt systems.

Guidelines:

1. Restrict unknown USB drives and downloads.
2. Install antivirus software on all devices.
3. Ensure school systems follow cyber hygiene standards.
4. Download apps only from trusted sources. Avoid clicking ads, pop-ups, or fake download buttons.

Response Procedures (SOP):

1. **Immediate Step:** Disconnect from the internet. Run antivirus scan.
2. **Remove malware:** and secure accounts. Reinstall the operating system if required.

Signs to Watch For

1. Device slowing down unexpectedly
2. Frequent pop-up ads
3. Apps crashing or freezing
4. Unauthorized access to accounts

Story: The Pop-Up Trouble

Meena was using her tablet to watch cartoons. Suddenly, many pop-up ads started appearing on the screen. The tablet became very slow, and apps kept closing by themselves.

Meena felt confused and told her teacher. The teacher explained that a **bad program called malware** had entered the tablet when Meena clicked a pop-up by mistake. With help from her parents, they cleaned the tablet and installed safety protection.

Meena learned to avoid pop-ups and download apps only from trusted places.

Classroom Message

If your device behaves strangely, stop using it and tell a trusted adult. It may have malware.

PART – F
RESPONSIBLY USING AI TOOLS

PART F: RESPONSIBLY USING AI TOOLS

Responsible use of AI means using smart tools—like chatbots, learning apps, or picture makers—in a safe and honest way. AI can help you learn faster, get new ideas, or make fun projects, but it should not do all your work for you. Always think for yourself! Don't share personal details like your name, school, phone number, or photos with AI apps. If AI gives you information, double-check it with a trusted adult or teacher because it can sometimes be wrong. Use AI only for good things—never to cheat, hurt others, or spread fake stories. And whenever you use AI in schoolwork, tell your teacher honestly. By using AI wisely, you can learn new skills and stay safe online.

This chapter for safe and ethical use of AI by adolescents, parents, and educators, aligned with India's emerging digital safety landscape based on India AI Governance Guidelines, Ministry of Electronics & Information Technology, Govt. of India.

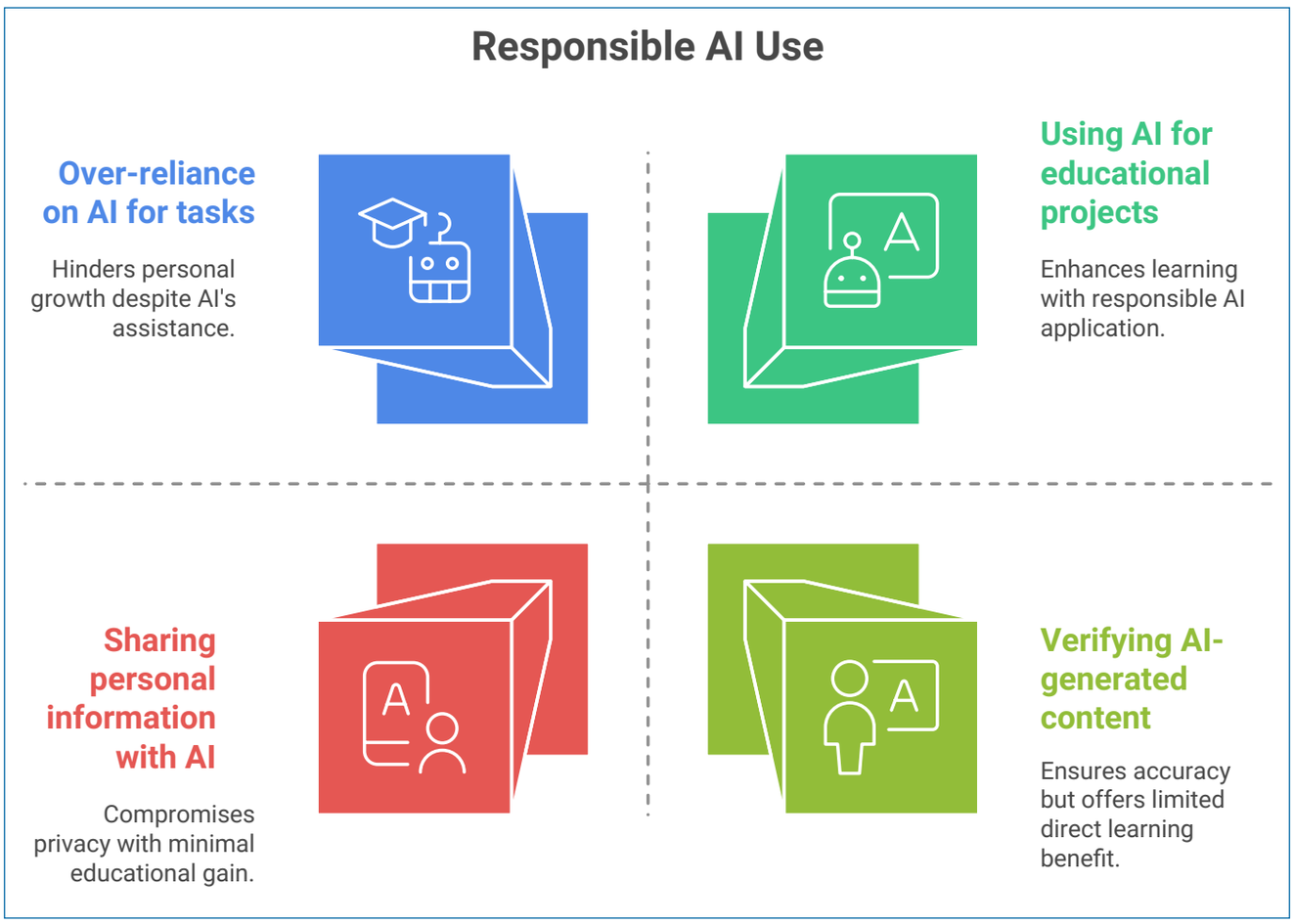


Figure 10: Responsible AI Use

Risks Associated with AI use by Adolescents

1. Misinformation & Wrong Answers

AI can sometimes give incorrect facts, made-up stories, or misleading explanations.

A student from Delhi asks an AI tool for "facts about the Revolt of 1857."
The AI wrongly states that it began in "Punjab in 1856" instead of Meerut in 1857.
If the student uses this in homework, it leads to wrong learning and poor academic performance.

2. Exposure to Harmful or Age-Inappropriate Content

AI tools can accidentally generate violent, sexual, hateful, or disturbing material.

A 13-year-old in Mumbai uses an AI image generator to create "cool superhero pictures."
The tool misinterprets the prompt and produces graphic or inappropriate images, exposing the child to harmful content.

3. Privacy Risks (Sharing Personal Information)

Many AI apps collect data. If adolescents input personal details, they may unknowingly share their identity, school name, photos, or location, which could be stored or misused.

A student enters, "Write a speech about my school ABC in a City A where I study in Class 8."
The student unknowingly shared his:
School name
Location
Age group
This information could be used by unsafe apps or unknown third parties.

4. Emotional Manipulation & Dependence

Some AI chatbots act like "friends," which can emotionally influence adolescents or lead to over-attachment.

A child in Bengaluru chats daily with an AI "friend bot."
They start sharing personal struggles, becoming dependent on the bot for emotional support.

This reduces real-life social connection and may expose them to harmful advice.

5. Academic Dishonesty (Cheating with AI)

AI can do entire assignments, essays, maths problems, coding projects, etc.These harms learning and can lead to disciplinary issues.

A Class 10 student in Faridabad uses an AI app to generate a full science project. The teacher notices the writing style is "too perfect," resulting in:

Academic penalties
Loss of trust
Weak understanding of science concepts

6. Overuse, Addiction & Reduced Critical Thinking

AI makes tasks easy—sometimes too easy—leading to over-reliance.

A student preparing for JEE stops practicing mathematic problems because the AI app instantly solves everything.

His problem-solving ability declines, and they lose confidence.

7. Creation of Fake or Harmful Content (Deepfakes & Misuse)

AI tools can generate fake images, voices, or videos of students—leading to cyberbullying, harassment, and reputational harm.

Students in a City Y school use an AI app to create a fake image of a classmate and share it in WhatsApp groups.

This becomes a case of image-based bullying, with emotional impact and potential legal consequences (POCSO, IT Act).

Responsible Use of Artificial Intelligence (AI) in Schools

The Directorate of Education mandates that all government, aided, and recognised private schools adopt age-appropriate and curriculum-aligned guidelines for the responsible use of Artificial Intelligence (AI) by students. AI-based tools must be used strictly for educational enhancement under the supervision of teachers and parents. Schools shall ensure that no student shares personal or sensitive information with AI platforms and that all AI-generated content is verified and supplemented with the student's original thinking.

Guidelines for Responsible AI Use for Students

- Use AI as a support tool, not a replacement for your own thinking.
- Never share personal information (name, school, photos, Aadhaar, location).
- Verify AI-generated content with books, teachers, or trusted websites.
- Avoid harmful prompts (violence, bullying, cheating, impersonation).
- Be honest—acknowledge when AI has been used in an assignment.
- Stay alert for unsettling or inappropriate outputs and report them.

Guidelines for Responsible AI Use for Parents

- Maintain open conversations about how AI tools work.
- Set clear rules for screen-time and AI use at home.
- Check the credibility and safety of AI apps used by the child.
- Monitor for sudden behavioural or emotional changes.
- Encourage your child to question and challenge AI-generated results.

Guidelines for Responsible AI Use for Educators and Schools

- Integrate AI literacy into ICT classes and life skills sessions.
- Maintain a vetted list of safe AI tools for classroom use.
- Clearly communicate rules on AI-assisted assignments.
- Teach students how to detect misinformation generated by AI.
- Establish a reporting mechanism for unsafe AI experiences

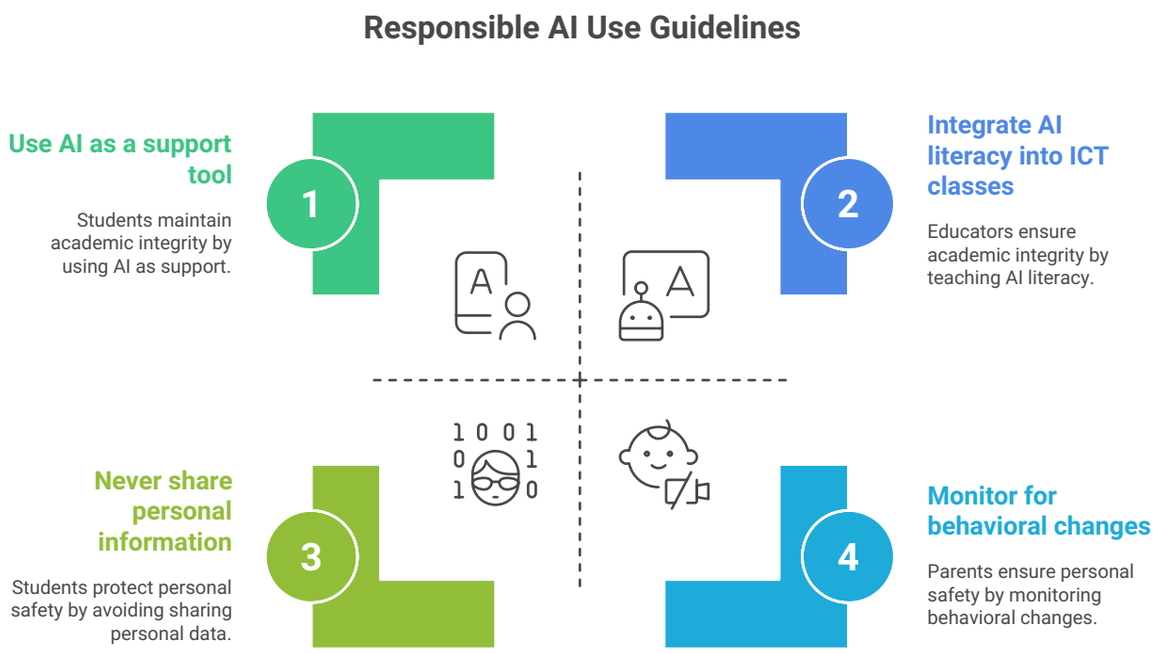


Figure 11: AI Use Guidelines

PART – G
CYBER-SAFE DESIGN STANDARDS

PART G: CYBER-SAFE DESIGN STANDARDS FOR SCHOOL APPS AND PORTALS

To ensure that any digital platform used by schools—such as learning apps, attendance portals, communication apps, ERP systems, parent dashboards, and homework platforms—follows uniform cybersecurity, data protection, and child-safety standards, thereby safeguarding students' personal information and preventing cyber risks.

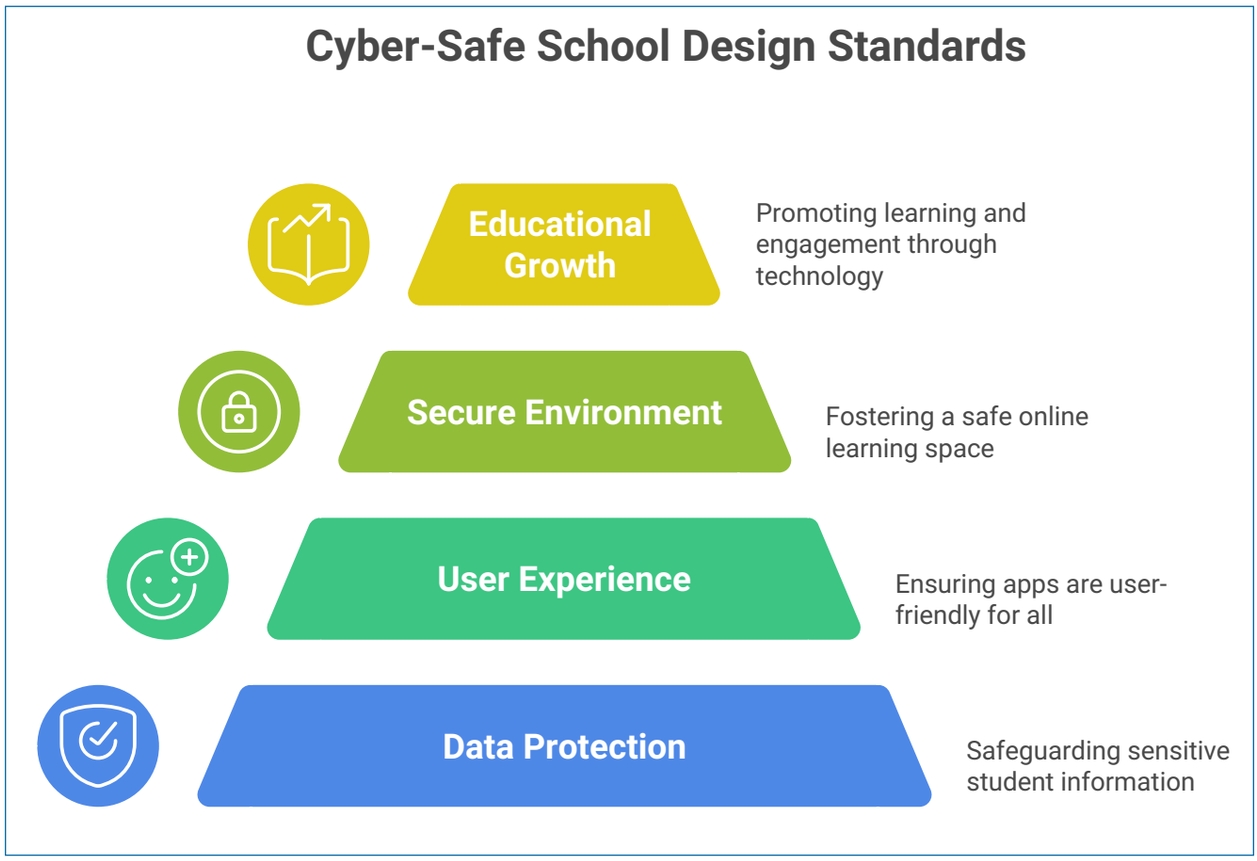


Figure 12: Cyber-Safe School Design Standards

Applicability

These standards apply to:

- School-run apps/portals
- Third-party EdTech tools used by schools
- Mobile apps for homework, attendance, fee payments, learning, communication
- Teacher-parent communication platforms
- Student performance tracking systems

Cyber-Safe Design Standards

Data Protection & Privacy Standards

Apps shall collect only what is strictly required:

- Name
- Class/Section
- Parent contact
- Attendance/academic records
- Aadhaar number, parent PAN, biometrics, photos if not required for essential functioning must not be collected.

Explicit Parental Consent[12]

As per the DPDP Act, 2023 consent from parents/guardians is mandatory before processing any data of student under 18.
Consent requests must be:

- Clear
- Separate (not bundled)
- Written in parent-friendly language

No Unauthorised Data Sharing

Apps must not share student data with:

- Third parties
- Advertisers
- Analytics companies
- AI model trainers

Unless explicitly approved by the school and parents and must be end-to-end encrypted.

[12]Refer Digital Privacy Data Protection Act (2023) and Digital Personal Data Protection Rules (2025)

PART – H
CYBER-SAFETY MOCK DRILL

PART H: ANNUAL CYBER SAFETY MOCK DRILL PLAN

An annual one-hour drill for all middle- and high-school students and staff to practice responding to cyber incidents (cyberbullying, phishing, fake profiles, etc.). The aim is to measure how quickly incidents are detected and reported, verifying that reports follow official channels, and assessing staff readiness to handle each scenario.

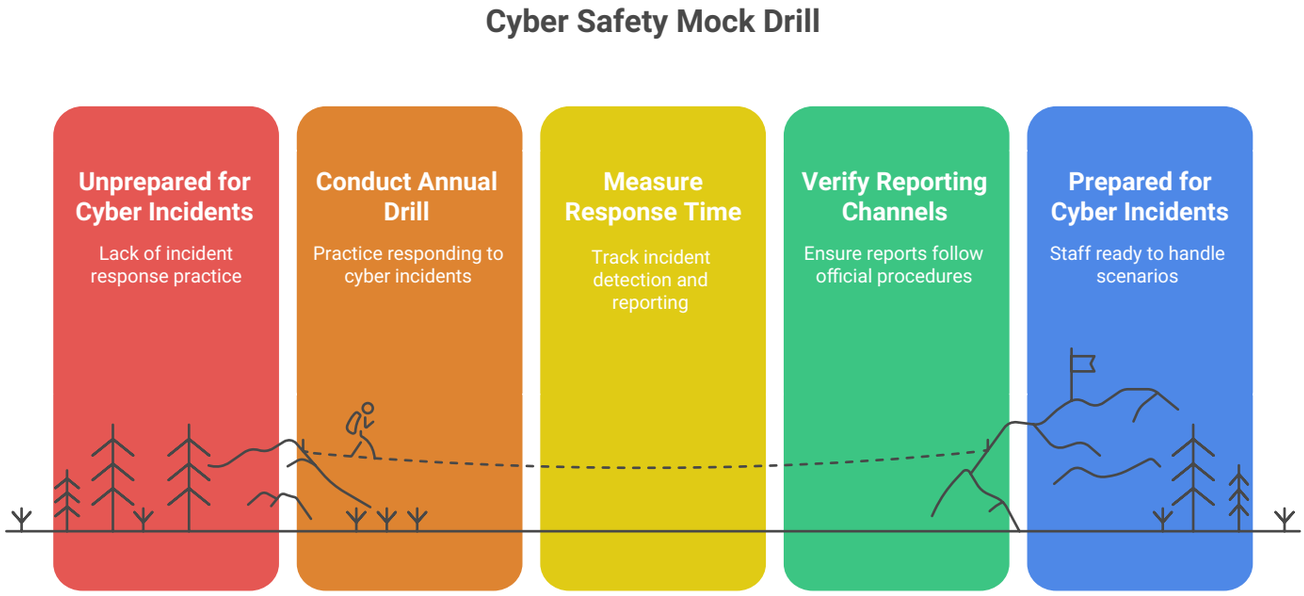


Figure 13: Cyber Safety Mock Drill

Participants & Preparation

- **Who takes part:**

  All students from Classes 6–12 and all school staff can join the drill. Teachers, IT staff, counsellors, and school leaders will help run it. One person—like the IT head, School Counsellor, or a teacher—can start the mock activities and keep track of what happens. Middle school students will get a little more guidance, while older students can respond more independently.

- **Before the drill:**

  The school can tell everyone the date and what kinds of cases will be practiced—like cyberbullying, phishing emails, or fake accounts. This way, no one gets scared or confused. The goal is to learn the correct steps, not to trick anyone. The school will also make sure the activity is safe, doesn't use real personal data, and doesn't cause any problems on real school systems.

- **What will be used:**

  The drill will use the school's regular online tools—email, learning apps, or class forums—to show pretend warning signs. Examples include a fake phishing email, a made-up social media post, or a

fake student profile. Teachers and observers will have simple forms to note what students and staff do and how quickly they respond, just like filling a report after a real incident.

Scenarios

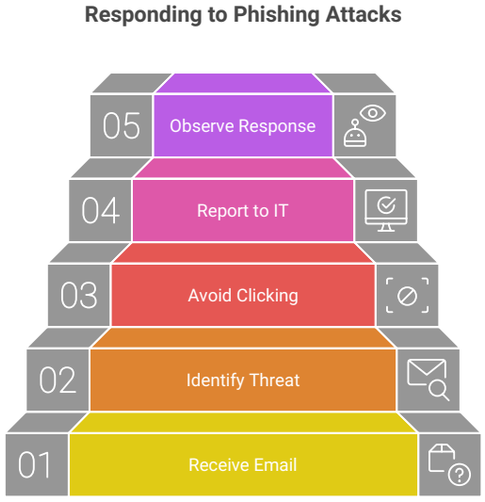
Design 3–4 tabletop or live scenarios, each lasting ~10–15 minutes. For each, outline roles and expected actions in advance (e.g. students are bystanders, staff must intervene).

Cyberbullying Case:

A pretend situation will show a student getting a hurtful or mean message on the class platform. The student should report it to a teacher or counsellor right away. The teacher will comfort the student, save the message as proof, and tell the right school leaders. Observers will check how quickly it was reported and if the message was saved properly.

Phishing Email Attack:

Everyone may receive a fake but harmless email trying to trick them—like "Click here to update your account." Students and staff should not click any links. Instead, they should report it to the IT team. Observers will note how many people spotted the fake email and how fast they reported it.



Fake Profile Incident

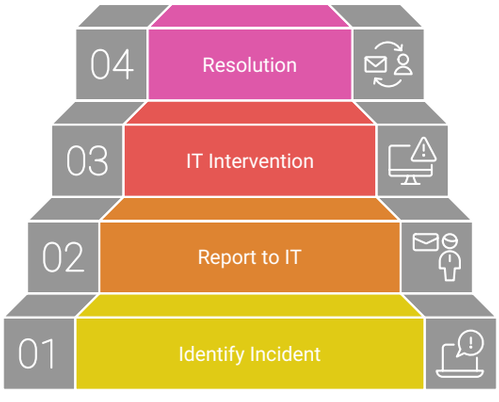
A pretend fake student or teacher account may appear on the school platform posting odd or inappropriate messages. Anyone who sees it should report it to a teacher or administrator. The staff will check if the profile is real, remove it, and inform others if needed. Observers will track how quickly this was noticed.

Responding to Fake Profile Incident

Other Possible Scenarios:

We may also pretend that an email account stops working or that a computer shows a fake "virus alert." Students and teachers should inform IT teacher immediately. The IT team will follow school steps to fix the issue safely. Observers will see how fast the problem is reported and handled.

Responding to Other Cyber Incidents



Evaluation Metrics & Checklists

Develop simple checklists/forms to evaluate each scenario, for example:

- Detection and Reporting: Did the target incident get reported? (Yes/No) By whom? How many people noticed before reporting? "Time to Report" – number of minutes from incident start to first report.
- Response Actions: List expected actions for each role (e.g. teacher: notify admin and document evidence; IT: warn others, block links; counsellor: support victim). Check off if each was done.

Figure 14: Cyber Drill Execution Plan

- **Chain of Command:** Verify whether reports followed the school's policy (e.g. Student→Teacher→Principal or email→IT helpdesk).
- **Communication:** Note if critical stakeholders were informed (e.g. parents, administrators, law enforcement if needed).
- **Resolution:** Was the issue contained (e.g. phishing link disabled, bully's account removed)?

For a post-drill report, compile an After-Action Summary:

1. **Incident Summary:** Describe each scenario and timeline (when it started, who responded, what actions were taken). Use the incident report template to "document what happened and how you responded".
2. **Metrics:** Include measured response times and rates (e.g. 5/10 staff reported phishing within 5 min). Highlight any bottlenecks (e.g. "Principal was not reached for 10 minutes").
3. **Observations:** List strengths (e.g. "Students immediately forwarded suspicious email to IT") and gaps (e.g. "Some teachers hesitated to escalate a social media incident"). This follows the advice to hold a debriefing where participants share experiences and note lessons learned.

4. **Recommendations:** Based on feedback, suggest improvements (e.g. update policy, conduct extra training, clarify reporting form).

After the Drill

- Debrief Discussion

Right after the drill, teachers and staff—and sometimes student leaders—will sit together for a quick discussion. They will talk about what went well, what was confusing, and how everyone reacted. This helps the school understand what needs to be improved for next time.

- **What Happens Next:**

The school will put all the notes and results into a simple report. This report will list what was learned, what needs fixing, and what actions will be taken. School leaders will use it to update the school's cyber safety rules and training. The goal is to keep everyone safer online by learning from the practice drill every year.

Sample Evaluation Checklist Items

(Example checklist/questions to adapt for each drill scenario)

- **Incident Detected:** (Y/N) Time reported: ____ min after start. Who discovered it?
- **Reporting Procedure Followed:** Was the incident reported to the correct person/office? (Y/N) – If not, note actual path.
- **Actions Taken:** List and check-off steps (e.g. evidence collected, account suspended, email attachment quarantined). Was each action done?
- **Communication:** Which stakeholders were informed (students, parents, admin, law enforcement)? Time of each notification.
- **Outcome:** Was the threat contained? Did any unintended issues occur?
- **Response Time:** Overall time from incident start to resolution. Compare against target (e.g. "All phishing attempts handled within 30 minutes" goal).

After filling out these items for each scenario, summarise in the post-drill report. This disciplined documentation will help the school show continuous improvement in cyber readiness.

PART – I
ROLES & RESPONSIBILITIES OF STAKEHOLDERS

PART I: ROLES & RESPONSIBILITIES OF STAKEHOLDERS

Staying safe online is something that everyone around children and adolescents want to encourage. The parents, caregivers, teachers, law enforcement agencies are there to guide, to talk and help you understand what is safe or unsafe on the internet.

Principal/ Head of school

Appoint a cyber safety security focal teacher, establish a school Cyber Safety *Committee*, ensure training plans are designed, staff training is conducted, and guidelines are implemented in these schools. Review all reported incidents.

Cyber safety security focal teacher (preferably ICT teacher)

Maintain the incident register, plan training sessions for teachers, organize awareness sessions in schools, act as first responder for online harm and liaise with police or child protection agencies if needed.

Teachers & staff

Take sessions on cyber safety with students and guide students in responsible use of internet.

Students

Follow the student code of conduct. Be kind, think before sharing and report unsafe behaviour.

School Counsellor / Health & Wellness Teacher/ EVGC Nodal

Provide psychosocial support and referral for affected students. Conduct group sessions on digital wellbeing.

Parents & Guardians

Attend orientation sessions, supervise home device use and encourage open conversations about digital safety.

I. Institutional Mechanisms and Action Points for Online Safety of Adolescents

1. Role of Schools as Focal Institutions

Schools shall act as the first line of prevention, response and capacity-building for online safety of adolescents. Given their daily engagement with students, schools are uniquely positioned to:

1. Build digital resilience and safe online behaviours;
2. Detect early warning signs of online harm;
3. Provide immediate support and reporting pathways;

4. Coordinate with parents, law enforcement, and child protection systems.

Note: All schools shall institutionalise online safety as a whole-school responsibility, not limited to IT teachers or counsellors.

2. Governance Structure at School Level

2.1. Constitution of School Cyber Safety Committee (SCSC)

Each school shall constitute a School Cyber Safety Committee (SCSC).

Composition:

1. Principal / Vice Principal – Chairperson
2. Designated Cyber Safety Nodal Teacher
3. School Counsellor / Psychologist
4. ICT / Computer Science Teacher
5. One Parent Representative (preferably PTA member)
6. Two trained Student Cyber Yodha Ambassadors (gender-balanced)

Key Responsibilities:

1. Oversee implementation of online safety guidelines;
2. Review cyber safety incidents and responses;
3. Approve awareness programmes and drills;
4. Liaise with external agencies (police, NGOs, helplines).

3. Preventive Mechanisms (Whole-School Approach)

Cyber Yodha Ambassadors Programme

Schools shall establish a Cyber Yodha Ambassadors Programme.

Objectives:

1. Build peer-to-peer awareness and support;
2. Encourage responsible digital citizenship;
3. Create early warning systems among students.

Roles of Cyber Yodha Ambassadors:

1. Promote safe online behaviour among peers;
2. Assist teachers during awareness sessions;
3. Encourage reporting and reduce stigma;
4. Act as student representatives in School Cyber Safety Committee.

For more details, please refer the Cyber Yodha Ambassadors Module.

II. Procedure for Response to Online Incidents

Step 1: Initial Disclosure and Triage

Initial disclosure is the first instance when a student, teacher, or parent reports or reveals a cyber-related concern or incident — such as cyberbullying, impersonation, data misuse, or online blackmail — to a trusted person within the school system on any working school day.

This moment is highly sensitive, as how the adult responds can determine whether the student feels safe, supported, and willing to proceed with further reporting.

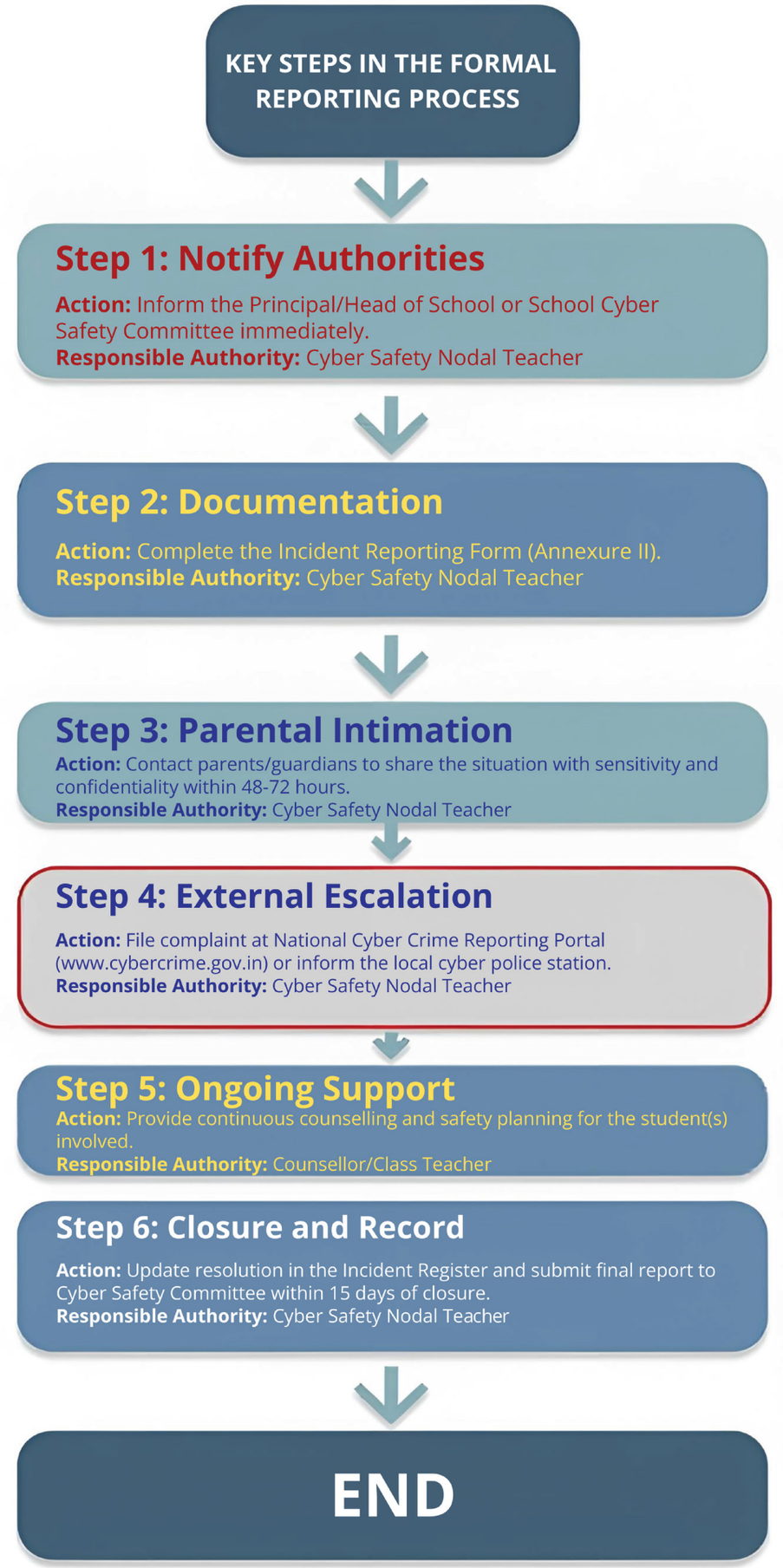
Step 2: Formal Reporting

This is the next critical phase after Initial Disclosure and Triage in a school's cyber safety system. Formal reporting is the structured documentation and official escalation of a cyber safety incident once the Initial Disclosure confirm that the case requires institutional or legal attention.

When Formal Reporting is Triggered

A case must move from Triage to Formal Reporting when it:

1. Involves potential criminal activity (e.g., cyberbullying, blackmail, grooming, hacking, or sexual exploitation);
2. Results in psychological or reputational harm;
3. Requires parental or legal authority involvement; or
4. Exceeds the school's capacity to resolve internally.


KEY STEPS IN THE FORMAL REPORTING PROCESS
Step 1: Notify Authorities
Action: Inform the Principal/Head of School or School Cyber Safety Committee immediately.
Responsible Authority: Cyber Safety Nodal Teacher
Step 2: Documentation
Action: Complete the Incident Reporting Form (Annexure II).
Responsible Authority: Cyber Safety Nodal Teacher
Step 3: Parental Intimation
Action: Contact parents/guardians to share the situation with sensitivity and confidentiality within 48-72 hours.
Responsible Authority: Cyber Safety Nodal Teacher
Step 4: External Escalation
Action: File complaint at National Cyber Crime Reporting Portal (www.cybercrime.gov.in) or inform the local cyber police station.
Responsible Authority: Cyber Safety Nodal Teacher
Step 5: Ongoing Support
Action: Provide continuous counselling and safety planning for the student(s) involved.
Responsible Authority: Counsellor/Class Teacher
Step 6: Closure and Record
Action: Update resolution in the Incident Register and submit final report to Cyber Safety Committee within 15 days of closure.
Responsible Authority: Cyber Safety Nodal Teacher
END

Support for Victim

1. **Counselling:** Immediately arrange for the adolescent to receive private, confidential counselling from the School Counsellor or an external mental health professional.
2. **Child Statement:** Ensure that, as per the POCSO Act, the child's statement is recorded in a child-friendly.
3. **Privacy:** Maintain absolute confidentiality regarding the victim's identity and the details of the incident. Only personnel involved in the investigation and support are to be informed.

Post-Incident Management

1. **Platform Reporting:** Immediately report the abusive profiles, links, or content to the respective social media platform (e.g., Instagram, WhatsApp, X) to ensure prompt removal. This can be done with the help of the district cyber police station.
2. **Periodic Review:** The School Cyber Safety Committee (CSC) must follow up with the IO (Investigating Officer) and the family, documenting the progress of the investigation and the child's recovery status.

Do's and Don'ts for Students:

1. **Do** stay calm and do tell an adult immediately. Report the incident to a teacher, parent or school counsellor right away.
2. **Do** keep evidence. Take screenshots of messages, posts or chats without altering them.
3. **Do** protect your privacy: use strong, unique passwords and keep your social accounts private. Only accept friend requests from people you know in real life.
4. **Do** treat others with respect online – be kind and "do understand what cyberbullying is and report any instances to a trusted adult".
5. **Don't** reply to or confront the bully. Engaging often makes the situation worse.
6. **Don't** share personal information (address, phone, school) with strangers.
7. **Don't** send compromising pictures or videos of yourself to anyone. Once something is sent, you can't control how it's used.

Do's and Don'ts for Teachers/Staff:

1. **Do** take every report seriously. Document the incident and collect evidence carefully. Follow the school's anti-bullying policy step by step.
2. **Do** inform other staff (principal, counsellor, Anti-Bullying Committee) so there is a coordinated response.
3. **Do** encourage the student by listening sympathetically and keeping them safe.
4. **Do** immediately notify parents (with the student's consent) if a serious incident occurs.
5. **Do** train students regularly on online safety and reporting methods.
6. **Don't** ignore warning signs or dismiss the student's fears. "Don't ignore signs of online distress" – intervening early is essential.
7. **Don't** try to manage a legal issue on your own. Once a complaint is made (or if the material is illegal), involve police.
8. **Don't** share students' personal details or photos on social media without consent, even innocently.

Do's and Don'ts For Parents/Guardians:

1. **Do** talk regularly with your child about their online life. Keep computers/devices in common areas. Make sure your child feels they can tell you anything without getting in trouble. Experts emphasize that "open communication with parents or guardians about online experiences is crucial".
2. **Do** set clear rules for internet use (time limits, approved apps/sites) and supervise younger children's activity.
3. **Do** respond calmly if your child comes to you. Thank them for telling you, and take action together. Let them know you believe them and will protect them.
4. **Do** seek help yourself. You can talk to school counsellors, or call helplines (below) for advice.
5. **Don't** panic or blame your child. Avoid shaming or threatening punishment for what happened. Remember the child is the victim.
6. **Don't** confront alleged perpetrators (their parents or peers) without guidance from school or police; always keep the school informed.

ANNEXURES

Annexures I : Response and Reporting Mechanism

Phase 1: Immediate Action – Securing Evidence (The First Hour)

The most critical step is preserving the evidence, as digital data is easily lost or deleted.

1. **Stop All Interaction:** Instruct the adolescent to immediately stop all communication with the alleged perpetrator. Do not reply, delete messages, or engage further.
2. **Secure the Evidence (Screenshot Everything)**
3. **Document Details:** Write down a detailed chronological account of the incident:
    - **Date and Time** the crime started and the last instance occurred.
    - **Platforms Used** (WhatsApp, Instagram, Telegram, Gaming Chat, etc.).
    - **Nature of the Crime** (Grooming, Sextortion, Cyberbullying, CSAM, etc.).
4. **Inform a Trusted Adult:** The adolescent must immediately inform a parent, teacher, school counsellor, or trusted relative. Under the POCSO Act, any adult who becomes aware of such an offense has a legal obligation to report it.

Phase 2: Formal Online Reporting (National Cyber Crime Portal)

This is the most efficient and recommended way to file an FIR (First Information Report) for cybercrimes in India. The case will be automatically routed to the Delhi Police Cyber Cell or the relevant police station.

Phase 3: Direct Reporting and Legal Channels

In addition to online reporting, use these direct channels for urgent, life-threatening, or time-sensitive matters.

A. Direct Police Contact (Physical Reporting)

B. Helpline Reporting

For immediate emotional support, guidance, or emergency intervention:

- **Child Helpline:** Call **1098**. This is a free, 24/7 emergency phone outreach service for children in need of care and protection. They can often provide immediate intervention and connect you with local authorities.
- **School Authorities:** Report the matter to the designated Child Protection Officer or School Counsellor. Schools have a mandatory reporting requirement under the POCSO Act

Annexure II : Incident Reporting Format

A standardized reporting form for recording, documenting, and addressing cyber incidents confidentially within schools.

Section A: Basic Information	
Field	**Details**
1. Date of Report:	
2. Name of School:	
3. Name of Reporting Person:	
4. Designation (Teacher / Student / Parent / Counsellor / Other):	
5. Contact Details (Phone / Email):	
Section B: Details of the Affected Student(s)	
Field	**Details**
1. Name of Student (Changed Name):	
2. Class & Section:	
3. Gender:	
4. Age:	
5. Parent/Guardian Name & Contact:	
Section C: Nature of Cyber Incident	
Category	**Tick (✓)**
1. Cyberbullying / Online Harassment	
2. Impersonation or Fake Profile	
3. Circulation of Obscene / Morphed Images	
4. Phishing / Hacking Attempt	
5. Identity Theft / Data Misuse	
6. Online Grooming or Exploitation	
7. Blackmail / Extortion	
8. Exposure to Harmful Content	
9. Other (Specify): _____	

Brief Description of the Incident:

(Include when, where, and how the incident was noticed or reported.)

Details of Evidence (if any):

Section D: Immediate Actions Taken	
Action	**Details/Date/Responsible Person**
1. Reported to Class Teacher / Counsellor	
2. Informed Principal / Cyber Safety Nodal Teacher	
3. Parent / Guardian Informed	
4. Counselling Support Provided	
5. Device / Account Secured	
6. Matter Reported to Cyber Cell / Police	
7. Complaint lodged on www.cybercrime.gov.in	
8. Report forwarded to Directorate of Education	
Section E: Outcome and Follow-up	
Field	**Details**
1. Resolution Status (Resolved / Pending / Referred):	
2. Date of Closure (if resolved):	
3. Remarks by School Cyber Safety Committee:	
4. Signatures:	
a. Principal / Head of School: _____	
b. Cyber Nodal Teacher: _____	

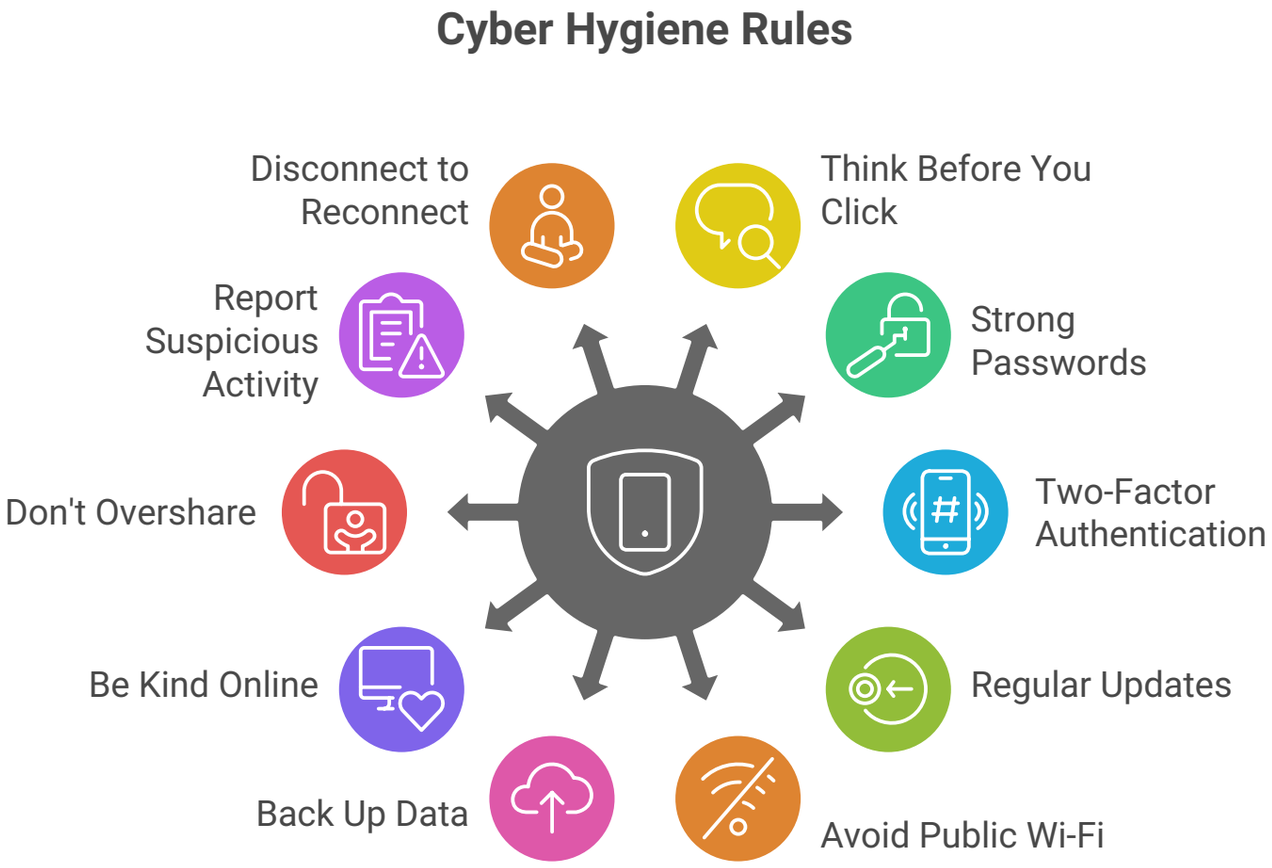
Confidentiality Clause

All information contained in this form shall be treated as strictly confidential and used only for official purposes in accordance with the school's Cyber Safety Guidelines SOP and child protection laws.

Annexure III : Cyber Safety Audit Checklist

Area	Indicators	Yes/No
1. School Cyber Safety Committee (SCSC) appointed	Notified by school, Designated and trained	
2. Focal Teacher appointed	Designated and trained	
3. Incident register maintained	Updated monthly	
4. Regular session on cybersecurity conducted	Monthly	
5. Cyber safety sessions conducted through external experts	Once per term	
6. Display of information on SCSC on school board	Updated	
7. Display of safety helplines on school board		
8. Students aware of reporting channels	Verified via survey	
9. Counselling sessions planned	Monthly	
10. School digital Infrastructure protected	Firewalls, antivirus, restricted Wi-Fi	
11. Parent sessions held	Bi-Annually	
12. Annual report submitted to DoE	Yes / No	

Annexure IV : Cyber Hygiene Golden Rules



Annexure V : Cyber Safety Pledge

Annexure VI : Resources and Support Systems

Organization / Helpline	Support Provided	Contact
National Cyber Crime Reporting Portal (MHA)	Online portal to report all types of cybercrimes.	cybercrime.gov.in
Indian Cybercrime Coordination Centre (I4C)	It works to fight cybercrime across the entire country.	https://i4c.mha.gov.in/
National Cyber Crime Helpline (MHA)	24×7 toll-free helpline guiding victims of cybercrime.	Tel: 1930 (toll-free)
Childline 1098 (Ministry of WCD)	24×7 free emergency helpline for any child in distress.	Tel: 1098 (toll-free)
Delhi Commission for Protection of Child Rights (DCPCR)	Helpline for children's rights and welfare issues in Delhi.	Tel: +91 9311551393
NCPCR – eBaalNidan Portal	National Commission for Protection of Child Rights (NCPCR) – grievance portal for child rights violations.	Website: https://eba alnidan.nic.in/)
National Commission for Women's Helpline (NCW)	24×7 toll-free helpline for women and girlsfacing harassment, violence or exploitation.	24×7 **Helpline: 14490**
Delhi Commission for Women (DCW)	24×7 toll-free helpline for women and girlsfacing harassment, violence or exploitation.	**Helpline: 181**

Annexures VII : List of Cyber Police Stations in Delhi

District	Office Address	Contact	Email ID
EAST	Cyber Police Station, Pandav Nagar, Near Trilokpuri Sanjay Lake Metro Station, Delhi-110091	6828401137	shocyber.east@delhipolice.gov.in
NORTH EAST	1st Floor, PS-Jyoti Nagar, New Delhi,110093	8750870788	cybercell.ned@delhipolice.gov.in
SOUTH	2nd Floor, PS- Saket, New Delhi-110017	8750870864	cybercell.south@delhipolice.gov.in
SOUTH EAST	2nd Floor, PS-Badarpur, New Delhi-110044	6828401537	cybercell.sed@delhipolice.gov.in
SOUTH WEST	Safdarjung Enclave, Opposite Rajendra Dhaba, New Delhi-110029	6828402537	shocyber.sw@delhipolice.gov.in
WEST	IInd Floor, PS Hari Nagar, New Delhi - 110064	011-25123432, 8750871174	shocyber.west@delhipolice.gov.in
OUTER	Police Post Mangolpuri, Patthar Market, Outer Ring Road, Pitampura New Delhi-110086	6828401837	shocyber.outer@delhipolice.gov.in
CENTRAL	Cyber PS Central District, Old Building, Kamla Market, New Delhi-110002	011-28210885, 6828401937	cybercell-central@delhipolice.gov.in
NORTH	Cyber Police Station/North ACP Operations Cell Office Complex, Behind Daulat Ram College, Maurice Nagar, Delhi- 110007	011-27666436, 6828402037	Cybercell-north@delhipolice.gov.in
NORTH WEST	2nd Floor, PS Model Town, Near Model Town Metro Station, New Delhi-110009	6828402137	cybercell-northwest@delhipolice.gov.in
SHAHDARA	2nd Floor, PS Shahdara, New Delhi-110032	6828401337	cybercell-shahdara@delhipolice.gov.in
ROHINI	Cyber Police Station, Sector -17, Rohini, New Delhi 110089	011-20879316	insp-cyber-rohini@delhipolice.gov.in
NEW DELHI	Cyber Police Station, PS Mandir Marg, New Delhi- 110001	011-23361880	shocyber.nd@delhipolice.gov.in
DWARKA	1st Floor, PS Dwarka North, Sec-17, Dwarka, New Delhi -110075	8287513200	shocyber.dwarka@delhipolice.gov.in
OUTER NORTH	Cyber Crime Police Station, Outer North District, Bawana, New Delhi- 110039	011-20875607, 7065036388	shocyber.on@delhipolice.gov.in
Source: https://cyber.delhipolice.gov.in/Districtcybercell.html			

Annexure VIII : List of Child Welfare Committees

S.No.	ChildWelfare Committee	Email-ID	District
1.	Child Welfare Committee-I, NirmalChhaya Complex, Hari Nagar, New Delhi.	cwc.ncc1@gmail.com	West
2.	Child Welfare Committee-II, Kasturba Niketan Complex, Lajpat Nagar, New Delhi	cwcsouthdelhi@gmail.com	South
3.	Child Welfare Committee-III, SewaKutir Complex, Kingsway Camp, Delhi	cwcsewakutirdelhi9@gmail.com	Central
4.	Child Welfare Committee-IV, NPS Building, Near Police Apartment, MayurVihar, Phase-I, Delhi	childwelfarecomtteemv@gmail.com	East
5.	Child Welfare Committee-V, Sanskar Ashram Complex, Dilshad Garden, Delhi	cwc5.sanskar.ashram@gmail.com	North East &Shahdara
6.	Child Welfare Committee-VI, Working Women Hostel Complex,Near Aman Vihar Police Station, Sector 22 Rohini, Delhi	cwc.northwestdelhi@gmail.com	North West
7.	Child Welfare Committee-VII Nirmal Chhaya Complex, Hari Nagar, New Delhi.	cwcsouthwest@gmail.com	South West
8.	ChildWelfare Committee-VIII, PWDBarracks, B- Block, Kalkaji, Delhi.	cwcsoutheastdelhi@gmail.com	South East
9.	Child Welfare Committee-IX, Community Centre, NPS Building, Near Police Apartment, Mayur Vihar, Phase-I, Delhi	delhicwc9@gmail.com	NewDelhi
10	Child Welfare Committee-X, Room No. 1 & 2, Building No. 5, Children Home for Boys, Opposite P.S. Alipur, Delhi	cwcalipur10@gmail.com	North

Annexure IX : List of District Child Protection Units (DCPUs)

S No.	DCPU & District	Name of DCPO	Address	Mobile
1.	DCPU-I (Central)	Ms. Parul	District Child Protection Unit-I, Central District, Sewa Kutir Complex, Kingsway Camp, Delhi	8802314408
2.	DCPU-II (North-East & Shahdara)	Ms. Anju Kumari	District Child Protection Unit-II, Room No. 10, Sanskar Ashram Complex, Dilshad Garden, Delhi.	9873023877
3.	DCPU-III (South)	Ms. Vasudha Singh	District Child Protection Unit-III, Kutir-5, Kasturba Niketan Complex, Lajpat Nagar-II, New Delhi.	9718817348
4.	DCPU-IV (West)	Ms. Sarita Kumar	District Child Protection Unit-IV, (WEST), Nirmal Chhaya Complex, Jail Road, Hari Nagar, Delhi.	8130601924
5.	DCPU-V (NorthWest)	Mr.ArunSharma	District Child Protection Unit-V, working Women Hostel,1st floor, Rohini Sector-22, Begumpur, Pkt 5, Near Aman Vihar Police Station	9911143645
6.	DCPU-VI (North)	Mr. Arunendra Narayan	District Child Protection Unit-VI, Room no. 3, Children Home for Boys-II, Alipur Opposite AlipurPolice Station, Delhi.	9899012315
7.	DCPU-VII (East)	Ms.Ritu	District Child Protection Unit-VII, Quarter no 32-33, Tower No 36, Kalyanwas Complex, Kalyanpuri, Dehi.	8744855034
8.	DCPU-VIII (South-East)	Ms. Anita Singh	District Child Protection Unit-VIII, Kutir No. 2, Kasturba Niketan Complex, Lajpat Nagar -II, New Delhi.	9650448603
9.	DCPU-IX (South West)	Ms. Sarita Kumar (Additional Charge)	District Child Protection Unit-IX, Nirmal Chhaya Complex, Jail Road, Hari Nagar, DELHI.	8130601924
10.	DCPU-X (Shahdara)	Ms. Anju Kumari	District Child Protection Unit-X, Shahdara	9873023877
11.	DCPU-XI (New Delhi)	Ms. Ritu	District Child Protection Unit-XI, Flat no.11, First Floor, Block No.2 Shankar Market, Connaught Place.	8744855034

Annexures X : Cybercrime Offences against Children and Applicable Indian Laws

Cybercrime Offences against Children and Applicable Indian Laws			
Cyber Issue	**Child-Friendly Explanation**	**Legal Meaning & Applicable Law (India)**	**Relevant Punishment**
Phishing	Tricking you online to steal passwords, OTPs, or money by pretending to be a trusted person or service.	BNS 2023 s.318 (Cheating), s.319 (Cheating by personation); IT Act s.66C, 66D	BNS: up to 7 years + fine; IT Act: up to 3 years + ₹1 lakh fine
Cyber Stalking	Someone repeatedly messages or follows you online even after you say "stop".	BNS s.78(1), 78(2)	1st offence: up to 3 years + fine; repeat: up to 5 years + fine
Cyber Bullying	Repeated online teasing, threats, or humiliation.	BNS s.75, s.78, s.351–356; IT Act s.66E, 67	Punishment varies: up to 3–5 years + fine depending on section
Identity Theft	Someone pretends to be you online using your photo, name, or account.	BNS s.319; IT Act s.66C	BNS: up to 5 years + fine; IT Act: up to 3 years + ₹1 lakh fine
Privacy Breach	Sharing someone's private photos or personal details without permission.	BNS s.77 (Voyeurism); IT Act s.66E, 72, 72A	BNS: 1–3 years (first), 3–7 years (repeat); IT Act: up to 3 years + fine
Unethical Hacking	Breaking into phones, games, or computers without permission.	IT Act s.66 read with s.43	Up to 3 years + ₹5 lakh fine (plus civil compensation)
Child Pornography / CSAM	Sexual images or videos involving children.	POCSO s.13–15; IT Act s.67B; BNS s.294–295	Minimum 3–7 years imprisonment + fine; repeat offences attract higher punishment
Online Grooming	An adult slowly builds trust online to exploit a child.	POCSO s.11(iv), 11(v)	Up to 3 years imprisonment + fine

Online Extortion / Sextortion	Threatening to share private photos unless money or favours are given.	BNS s.308 (Extortion); s.351–356	Up to 10 years imprisonment + fine
Digital Payment Scam	Losing money through fake links, QR codes, or OTP fraud.	BNS s.318, s.319; IT Act s.66C, 66D	BNS: up to 7 years + fine; IT Act: up to 3 years + ₹1 lakh fine
Sexting (Minors)	Any sexual image, video, or message involving a child—even if shared willingly.	POCSO s.13–15; IT Act s.67B	Minimum 3–7 years imprisonment + fine
Online Child Sexual Abuse & Exploitation	Sexual harm to a child using the internet, games, or social media.	POCSO s.3–15; IT Act s.67B; relevant BNS sexual offences	Severe punishment: rigorous imprisonment, may extend to life imprisonment, plus fine
Online Trafficking	Using social media or the internet to trap or exploit people for labour, marriage, begging, or sexual abuse.	Trafficking of Persons Act s.31–33, 36, 41; BNS s.143–146; POCSO (if child involved)	Minimum 10 years to life imprisonment + fine; aggravated if digital platforms used

Annexures IX : Real-Life Examples

15-year-old girl a victim of cyberstalking

A 15-year-old adolescent girl from Delhi who became a victim of cyberstalking and online sexual harassment. The accused, a 34-year-old man named Akhilesh Kumar, created fake profiles and relentlessly harassed her on social media. The adolescent was stalked by an individual she met on Facebook, with whom she had shared personal and sensitive information including her phone number. After unfriending him on the platform due to discomfort, the stalker created a fake profile using her photos and personal details, further harassing her online.

Blue Whale Challenge

The Blue Whale Challenge was an alleged online game rumoured to encourage vulnerable adolescents to complete a series of dangerous tasks, culminating in self-harm or suicide. This phenomenon created widespread fear among parents, educators, and children across India, amplified heavily by sensational news reports and social media discussions.

Image Morphing

The Bois Locker Room incident, which surfaced in May 2020, was a significant case highlighting the misuse of digital platforms by minors to objectify and threaten underage girls. The controversy centred around an Instagram group chat where male students shared morphed images of female classmates and discussed sexually explicit content, including threats of rape.

Academic Decline

A 16-year-old boy from Bengaluru named Arjun developed a severe addiction to online gaming and social media platforms, spending over 10 hours daily on his smartphone. Initially, his parents noticed academic decline and loss of interest in outdoor activities and family time. As the addiction deepened, Arjun began experiencing sleep deprivation, irritability, and withdrawal symptoms when separated from his digital devices.

REFERENCES

A Handbook for Adolescents/Students on Cyber Safety, Ministry of Home Affairs, GoI

https://bit.ly/4peHSB0

Artificial Intelligence Integration for School Curriculum, CBSE

https://bit.ly/4qq5TGh

Child Online Protection in India, UNICEF

https://bit.ly/3MVYdx4

Cyber Safety Booklets for Adolescents, CBSE

https://bit.ly/4poN5Xi

Deepfake Technology in India and World: Foreboding and Forbidding

https://bit.ly/4q3Pl7u

Digital Personal Data Protection (DPDP) Act & compliance requirements for processing minors' data.

https://bit.ly/3YKbUBN

Guidelines on School Safety and Security, Department of School Education & literacy, Ministry of Education, Govt. India

https://bit.ly/3YxVjRX

Guideline and standard content for raising awareness among children, parents, educators and general public titled "Being Safe Online"

https://bit.ly/4jltwxE

Guidelines on Cyber Safety (for inclusion in) Manual on Safety and Security of Children in Schools

https://bit.ly/4qq5Qu5

Guidelines for Schools for prevention of bullying and cyber bullying

https://bit.ly/4pwNdnH

Government's measures to ensure safe and accountable internet

https://bit.ly/4qxZwAZ

Handbook on Digital Safety for Children, NCERT

https://bit.ly/4jeXWl5

Ministry of Education guidance on introducing AI curriculum in schools https://bit.ly/4qrtZ3q

MeitY / India AI Governance Guidance

https://bit.ly/4jfMMw9

Online Safety for Children: Protecting the Next Generation from Harm, NITI Aayog

https://bit.ly/4jgdMMg

Steps taken by Government of India to address the issue of addiction of children to online games

https://bit.ly/3YfTYyV

Directorate of Education
Govt. of NCT of Delhi

Cyber NISHTHA

Guidelines on Cyber Safety for Adolescents