MATRI SUDHA
(A Charitable Trust)

# Are Adolescents Equipped for Breaking the Cyber Chakravyuh?

## (A Report on Risks, Responsibilities and Resolutions in India's Digital Age)

# CONTENTS

सत्यमेव जयते

# OFFICE OF THE MINISTER

## MINISTER OF HOME, POWER, URBAN DEVELOPMENT, EDUCATION, HIGHER EDUCATION, TRAINING & TECHNICAL EDUCATION GOVT. OF NATIONAL CAPITAL TERRITORY OF DELHI

No./Minhom/1041402

Dated : 29/09/25

**FOREWORD**

Adolescents represent one of India's greatest strengths and a vital foundation for our nation's future. With nearly one in five Indians in this age group, their wellbeing, safety, and preparedness to engage with an increasingly digital world is of utmost importance.

Today's young people are growing up in an era where technology is woven into every aspect of their lives—be it education, social interaction, entertainment, or financial activity. While digital platforms offer immense opportunities for learning and innovation, they also expose adolescents to risks such as online harassment, misinformation, fraud, exploitation, and breaches of privacy. Navigating this complex digital terrain requires not only access, but also awareness, critical thinking, and resilience.

The Government has already initiated several measures to strengthen cyber safety and digital literacy, including the Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal, and school-based awareness programmes. Yet, community-based studies and partnerships remain equally important in building a culture of safe and responsible digital engagement.

In this context, I am pleased to introduce this research study on Online Digital Safety for Adolescents undertaken by Matri Sudha. The study sheds light on the realities faced by adolescents in the digital space, while also offering insights for parents, teachers, and policymakers. Such efforts are essential in shaping an ecosystem where our children and adolescents are protected, informed, and empowered.

I extend my appreciation to Matri Sudha for their commitment to this important issue. I trust this work will contribute meaningfully to ongoing discussions and policy initiatives, and will inspire collective action to ensure that the digital world becomes a place of opportunity rather than vulnerability for our young citizens.

**(ASHISH SOOD)**

A-Wing, 7th Level, Delhi Secretariat, I.P. Estate, New Delhi-110002
Tel. No.:23392116, 23392117 Email : min-hep@delhi.gov.in

**REKHA SHARMA**
**MEMBER OF PARLIAMENT**
**(RAJYA SABHA)**
Former Chairperson : National Commission for Women

सत्यमेव जयते

Flat No.1, GF, Tower - 5, Type-7,
East Kidwai Nagar, New Delhi - 110023
E-mail : sharmarekha.63@sansad.nic.in

# Foreword

India today has one of the largest populations of adolescents in the world. This demographic dividend can only be fully realized if our young citizens are safe, empowered, and responsible in the digital ecosystem. However, the rapid expansion of social media, online gaming, financial technology, and artificial intelligence has also exposed adolescents to cyberbullying, misinformation, financial frauds, exploitation, and privacy violations. The digital space, much like the ***Chakravyuh*** of our epics, demands not only courage but also the knowledge, skills, and resilience to navigate safely.

The Government of India has taken several steps in this direction, including the establishment of the Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal, and digital literacy programmes across schools.

It gives me immense pleasure to present the foreword to this important research study on *Online Digital Safety for Adolescents*, prepared by **Matri Sudha**. In an era where the digital world has become inseparable from our daily lives, young people—our adolescents—find themselves at the heart of unprecedented opportunities as well as emerging risks.

I commend Matri Sudha for taking up this timely initiative. I am confident that this study will serve as a valuable resource for policymakers, educators, and practitioners working to protect and empower our adolescents in the digital age.

As we move forward, let us reaffirm our collective responsibility: to safeguard our youth, to equip them with the tools to thrive in a digital society, and to ensure that technology remains an instrument of progress, not peril.

**Rekha Sharma**

# Foreword

The research study on *Online Digital Safety for Adolescents*, prepared by Matri Sudha, is an important piece of information.

The metaphor of the *Chakravyuh* from our epics is a befitting reminder of its relevance even in the present digital age. For adolescents today, the internet offers unprecedented opportunities for learni ng, communication, and creativity. Yet, it also presents hidden dangers—cyberbullying, online exploitation, financial frauds, identity theft, and exposure to harmful content. Navigating this digital maze requires knowledge, awareness, and resilience.

Through initiatives such as regular outreach programmes in schools and communities, we strive to ensure that technology remains a tool for empowerment rather than exploitation.

I am confident that this report will serve as a valuable resource for policymakers, law enforcement agencies, educators, technology platforms, parents, and adolescents alike.

Rajneesh Gupta
Joint Commissioner of Police
IFSO (Cyber Crime Unit), Delhi Police

**VEDITHA REDDY, IAS**
Director, Education & Sports

सत्यमेव जयते

Directorate of Education
Govt. of NCT of Delhi
Room No. 12, Old Secretariat
Near Vidhan Sabha,
Delhi-110054
Ph.: 011-23890172
E-mail : diredu@nic.in

## MESSAGE

It gives me pleasure to express my thoughts for the research study on Online Digital Safety for Adolescents, prepared by Matri Sudha. This report addresses an issue that is of profound significance in today's educational landscape, where the boundaries between the physical and digital worlds are increasingly blurred.

For our adolescents, the digital space is no longer a distant concept, it is an integral part of their learning, socialisation, and self-expression. While this environment brings opportunities for creativity, knowledge, and connection, it also presents unique risks such as cyberbullying, online exploitation, misinformation, and privacy violations. The challenge before us-as educators, policymakers, parents, and society at large is to ensure that our students can embrace the benefits of the digital age without falling prey to its perils.

The Directorate of Education, Government of NCT of Delhi, has consistently prioritised the well-being and holistic development of our students. We recognise that digital literacy and online safety must now be central to this vision. Initiatives in schools have begun to integrate awareness on cyber safety, resilience, and responsible digital behaviour. However, there is a pressing need for stronger evidence, deeper engagement, and collective action to safeguard our adolescents in this complex environment.

As we move forward, let us reaffirm our shared commitment: to equip every adolescent not only with knowledge and skills, but also with the resilience and confidence to navigate the digital world safely and responsibly.

**(VEDITHA REDDY, IAS)**

चन्दन कुमार चौधरी
विधायक, संगम विहार
दिल्ली विधान सभा

सत्यमेव जयते

**Chandan Kumar Choudhary**
Sangam Vihar, Delhi
Member of Legislative Assembly of Delhi
Govt. of National Captial Territory of Delhi

**Foreword**

**Date :** 23/09/2025

India today stands at a defining juncture, where the energy and aspirations of one of the world's largest adolescent populations hold the key to our nation's progress. This demographic dividend can only be fully realized if our young citizens remain safe, empowered, and responsible while engaging in the fast-expanding digital ecosystem.

While technology has opened doors of learning, communication, and innovation, it has also exposed adolescents to alarming risks—cyberbullying, misinformation, financial fraud, privacy breaches, and the growing menace of online gaming addiction. Recognizing these threats, the Government of India has taken concrete steps, including the establishment of the Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal, digital literacy programmes in schools, and regulatory measures to curb harmful online gaming practices. The recent restrictions on dangerous and addictive online games are a strong step toward ensuring the well-being of our youth.

The digital space is not without challenges—it is much like the Chakravyuh of our epics, requiring not just courage, but knowledge, skills, and resilience to navigate safely. I wish to caution adolescents and parents alike: reckless use of digital platforms can put health, education, finances, and even personal safety at serious risk. Awareness, self-discipline, and timely reporting of suspicious activities are essential to prevent exploitation and harm.

It gives me immense pleasure to write this foreword for the important research study on Online Digital Safety for Adolescents, prepared by Matri Sudha. At a time when technology has become inseparable from our daily lives, this study will serve as a valuable resource for policymakers, educators, and practitioners who are committed to safeguarding the interests of our young generation.

I sincerely commend Matri Sudha for taking up this timely initiative and for their dedication toward empowering our adolescents. Together, we must reaffirm our responsibility: to protect our youth, to equip them with digital literacy, and to ensure that technology becomes a tool for growth and empowerment, not a cause of distress or danger.

Shri Chandan Kumar Choudhary

MLA, Sangam Vihar

Delhi Legislative Assembly

Chairman, Committee on Peace & Harmony, Delhi Legislative Assembly

**Mob. : +91-9953137979 | Email : chandankrchaudharymla@gmail.com**
**Office : G-2, 18/44, Ratiya Marg, Sangam Vihar, New Delhi - 110080**

# *Acknowledgment*

Matri Sudha is grateful to all the adolescents who shared their voices and experiences, making this report – *Are Adolescents Equipped for Breaking the Cyber Chakravyuh*?Their valuable experiences and perspectives, enabling us to understand the challenges and opportunities of navigating the digital world. Their voices form the heart of this report.We also thank parents, teachers, school authorities, child welfare committees, and cyber police officials for their valuable insights.

**Adv. Arvind Singh**
**Technical Head & Advisor**
**Matri Sudha**

Our sincere appreciation goes to Shri Ashish Sood, Hon'ble Minister of Education, Govt. of NCT of Delhi; Smt. Rekha Sharma, Hon'ble Member of Parliament (Rajya Sabha) & Former Chairperson – National Commission for Women; Sh. Rajneesh Gupta, Joint CP/I.F.S.O., Special Cell, Delhi Police; Smt. Veditha Reddy, Hon'ble Director, Directorate of Education & Sports, Govt. of NCT of Delhi; Sh. ChandanKumar Choudhary, Hon'ble MLA, Sangam Vihar and Chairperson, Committee on Peace & Harmony (Delhi Vidhan Sabha); Dr. Vikram Srivastava, Founder, Independent Thought; Mr. Varun Pathak, Child Rights Expert; Mr. Ravi Shanker Rai, Executive Board Member, Matri Sudha; Advocate Sakshi Rewaria, Faculty of Law, Indian Institute of Management, Rohtak, Haryana; Rise Up India for their valuable guidance and giving shape to this report. I also extend my gratitude to all partner organizations (Saksham, Navsrishti, Jamghat, SPID and Saksham Foundation) and all the volunteers who helped in the data collection.

This report is dedicated to adolescents, with the hope of contributing to safer and more empowering digital spaces for them.

Jai Hind, Jai Bharat!

# *Executive Summary*

**Emerging Risks, Responsibilities and Resolutions**

India today has one of the world's largest populations of children and adolescents online, with more than 400 million minors accessing the internet through smartphones, ed-tech platforms, and social media. While digital connectivity has expanded learning and social opportunities, it has also exposed children to unprecedented risks: cyberbullying, grooming, deepfakes, misuse of personal data, addictive gaming, and exposure to harmful or exploitative content.

The digital ecosystem has become central to the lives of adolescents in Delhi, shaping how they learn, socialize, and express themselves. With the expansion of smartphones, affordable data, and digital education platforms, adolescents now spend more time online than any previous generation. However, this digital immersion presents a paradox—while it creates opportunities for growth and empowerment, it also exposes young people to a complex web of risks. This study conceptualizes the online world as a **Cyber Chakravyuh**—a labyrinth of emerging risks, competing responsibilities, and the urgent need for multi-level resolutions.The metaphor of *Cyber Chakravyuh* aptly illustrates the digital environment of adolescents in Delhi—complex, layered, and difficult to exit once risks are encountered without prior preparation. Like the mythological Chakravyuh, adolescents often enter the digital maze with enthusiasm but without adequate knowledge of safe pathways.

Recognizing the online world as a *Cyber Chakravyuh* draws attention to the urgent need for collective responsibility—by adolescents, their families, schools, policymakers and law enforcement agencies—in ensuring that the promise of digital technology translates into safe, equitable, and empowering experiences for all.

# Chapter 1: Introduction

The digital revolution has redefined childhood and adolescence across the globe. In India, and particularly in Delhi as the national capital, the presence of affordable smartphones, inexpensive internet access, and rapid digitization of education and services have placed adolescents at the center of a profound transformation. Adolescents today are not just passive consumers of digital technologies—they are active creators, influencers, learners, and decision-makers in the online space.

Delhi has one of the highest internet user bases in India. This widespread access, while beneficial, means that a larger portion of the population, including those with varying levels of digital literacy, are exposed to online spaces without adequate protection.The demographic profile of Delhi includes a vast number of children and youth who are often "digital natives." This generation is comfortable with technology but may lack the critical awareness to identify and mitigate risks like cyberbullying, online grooming, and misinformation in the form of cybercrimes.

Yet, this digital inclusion comes with an inherent paradox. While the internet provides unprecedented opportunities for self-expression, learning, and socialization, it also exposes adolescents to a spectrum of risks that are often invisible, pervasive, and difficult to manage.

This duality has created what can be described as a Cyber Chakravyuh—a complex labyrinth of digital interactions where entry is easy, but navigating through risks and exiting safely requires skill, preparation, and support.Data from various sources, including the National Crime Records Bureau (NCRB) and specific academic studies, indicates a worrying trend of rising cybercrimes in India, with urban areas like Delhi being key hotspots.Adolescents are at higher risks of cyberbullying, exposure to inappropriate content, and online grooming by predators. The UNICEF-commissioned report "Child Online Protection in India,

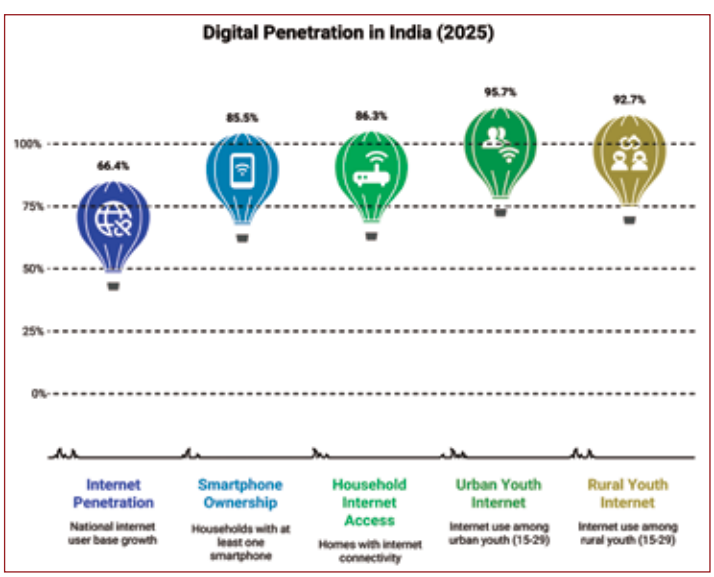



*Figure 1: Comprehensive Modular Survey: Telecom, 2025*

- **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)

2016" highlights that while digital access is increasing, a lack of digital literacy and online safety measures exposes children to hazards like cyber-bullying and sexual predation.

According to National Crime Records Bureau (NCRB) the nnationwide in 2022, there were 162,449 crimes against children, up by 8.7% from the previous year. The dominant categories were kidnapping/abduction (45.7%) and POCSO (39.7%), which includes child sexual abuse. In 2022, Delhi registered 1,529 POCSO cases. Cybercrime cases for all categories in Delhi in 2021 were 345, in 2022, in 2023 there were 685 cybercrime 2024, 755 cybercrime complaints were registered.According to Central Reserve Police Force Cyber Byte's (2024) Cyberattacks on India are projected to rise to a staggering 1 trillion per annum by 2033, reaching 17 trillion by 2047.

Various researches indicate a significant gap between the number of people who experience online harm and those who actually report it. This is often due to a lack of awareness about reporting mechanisms, procedural difficulties, and a deep-seated mistrust in institutional support. A 2025 Lokniti-CSDS survey in Delhi found that while 93% of respondents were aware they could file a complaint, only 21% of those who experienced a cybercrime actually reported it to the authorities. Law enforcement agencies, despite initiatives like dedicated cyber police stations, often face challenges with the scale and technical complexity of cybercrimes. A lack of specialized training, inadequate resources, and insufficient legal provisions for certain types of online harassment contribute to low conviction rates.

On the other hand, there are societal attitudes towards online harassment which act as a major barrier in reporting. Victims, particularly women and girls, may face victim-blaming or a lack of familial support, which prevents them from coming forward. Cultural norms around privacy, sexuality, and reputation make these crimes particularly difficult to address publicly, as detailed in various studies on the socio-cultural factors affecting online safety in India.

# Chapter 2: Understanding Cybercrimes

Cybercrime is any activity involving a computer, network, or networked device for criminal means. It's a serious global threat on the rise that affects individuals, businesses, society, and governments. Cybersecurity Ventures projects that cybercrime will cost the world $8 trillion in 2023 and $10.5 trillion by 2025.What's more concerning is the human trafficking component. Victims, including Indian nationals, are being lured abroad with fake job offers and then forced into cybercrime rings. These trafficked individuals are made to impersonate government officials, police officers, or financial advisors to con unsuspecting Indians

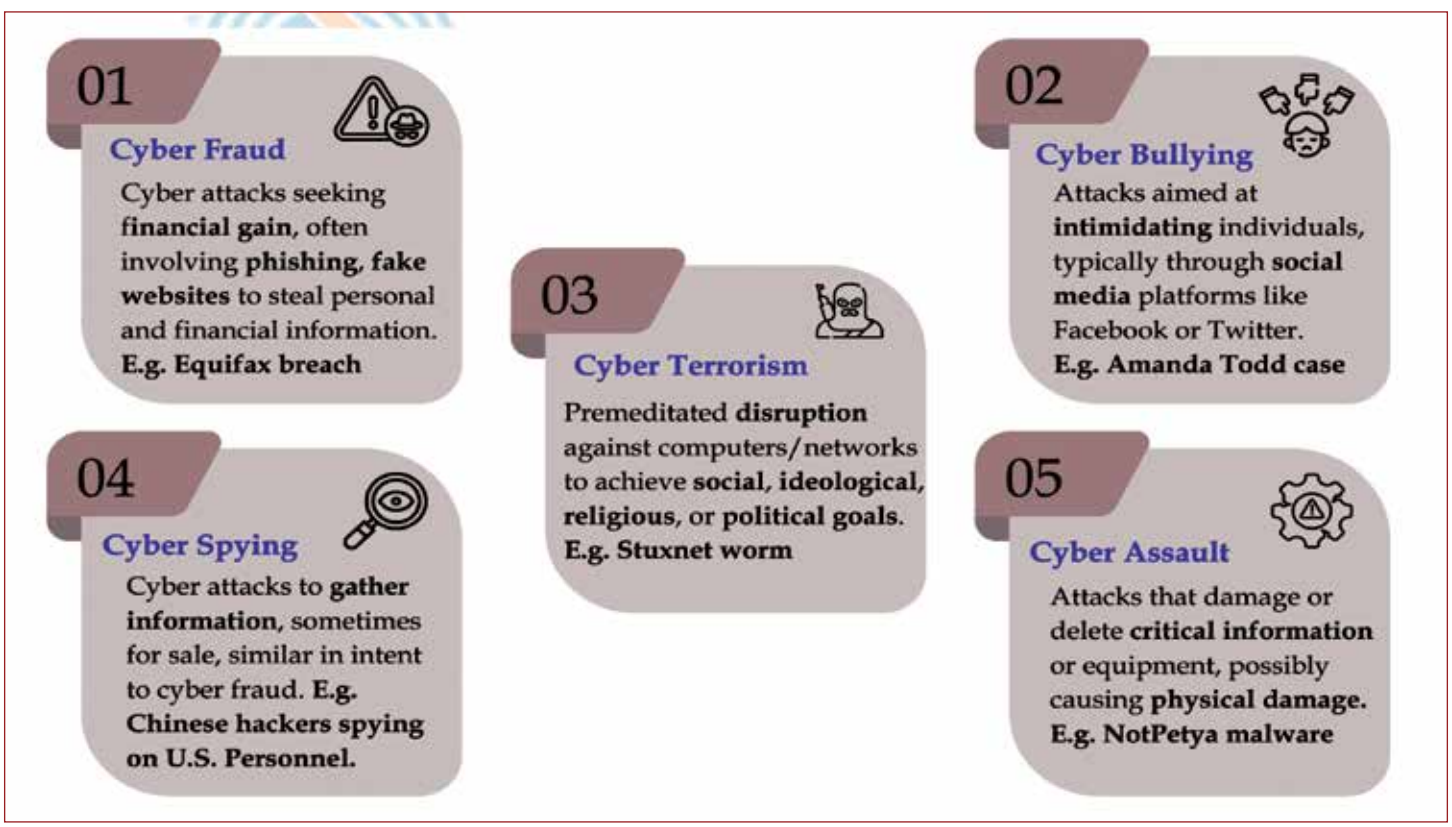



*Figure 2: Rising cybercrimes in India, Ministry of Home Affairs, GoI*

**Factors responsible for the increasing vulnerability to cybercrimes in India**

1. Rapid digitalization: Digital transactions in India reached $1.2 trillion in 2023, according to the RB, creating more opportunities for cybercriminals.
2. Large internet user base: India has the second-largest internet user base globally, making it a lucrative market for cyberattacks.
3. Low levels of digital literacy: Only 38% of Indian households are digitally literate.

- Digital divide: Digital literacy is higher in urban areas at 61%, compared to 25% in rural areas.

4. Inadequate cybersecurity infrastructure: A recent study by Cloudflare has revealed that 83% of Indian organizations experienced at least one cybersecurity incident in 2022[1].

[1]*Rising cybercrimes in India, Ministry of Home Affairs, GoI*

## 2.1. Current Cybersecurity Framework in India

**Legislative Framework:**

- The Information Technology (IT) Act, 2000: It is the primary legislation dealing with National Cyber Security Policy, 2013: cybersecurity, data protection and cybercrime.
- `This was the first major step by the Indian government towards creating a secure cyberspace ecosystem. It focuses on:
  - Protecting information infrastructure in cyberspace.
  - Reducing vulnerabilities and building capabilities to prevent and minimize damage from cyber incidents.
  - Developing a combination of institutional structures, people, processes, technology, and cooperation to enhance cybersecurity.
- National Cyber Security Strategy 2020: Developed by the National Security Council Secretariat, its pillars are:
  - Secure: Protecting the national cyberspace.
  - Strengthen: Enhancing structures, people, processes, and capabilities.
  - Synergise: Fostering resources, cooperation, and collaboration.

**Institutional Framework:**

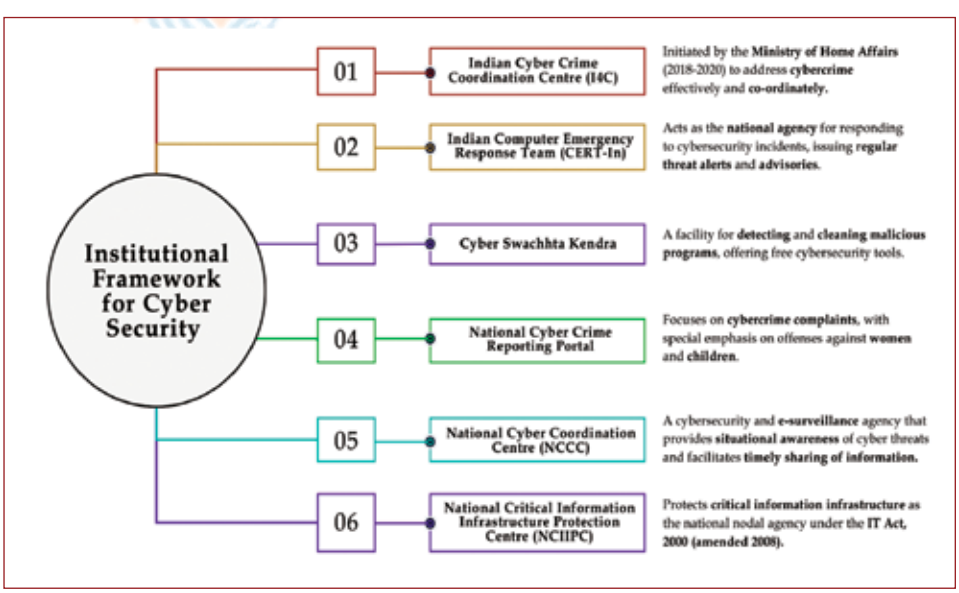



*Figure 3: Rising cybercrimes in India, Ministry of Home Affairs, GoI*

## 2.2. How to report a suspect of cyber fraud?

### 2.2.1.Sanchar Saathi

Sanchar Saathi is a citizen centric initiative launched by the Department of Telecommunications (DoT), Government of Indiaon 16 May 2023 to empower mobile subscribers, strengthen their security and increase awareness about citizen centric initiatives of the Government. Sanchar Saathi is available in form of Mobile App and web portal (www.sancharsaathi.gov.in). Sanchar Saathi provides various citizen centric services.

**Key features of Sanchar Saathi**

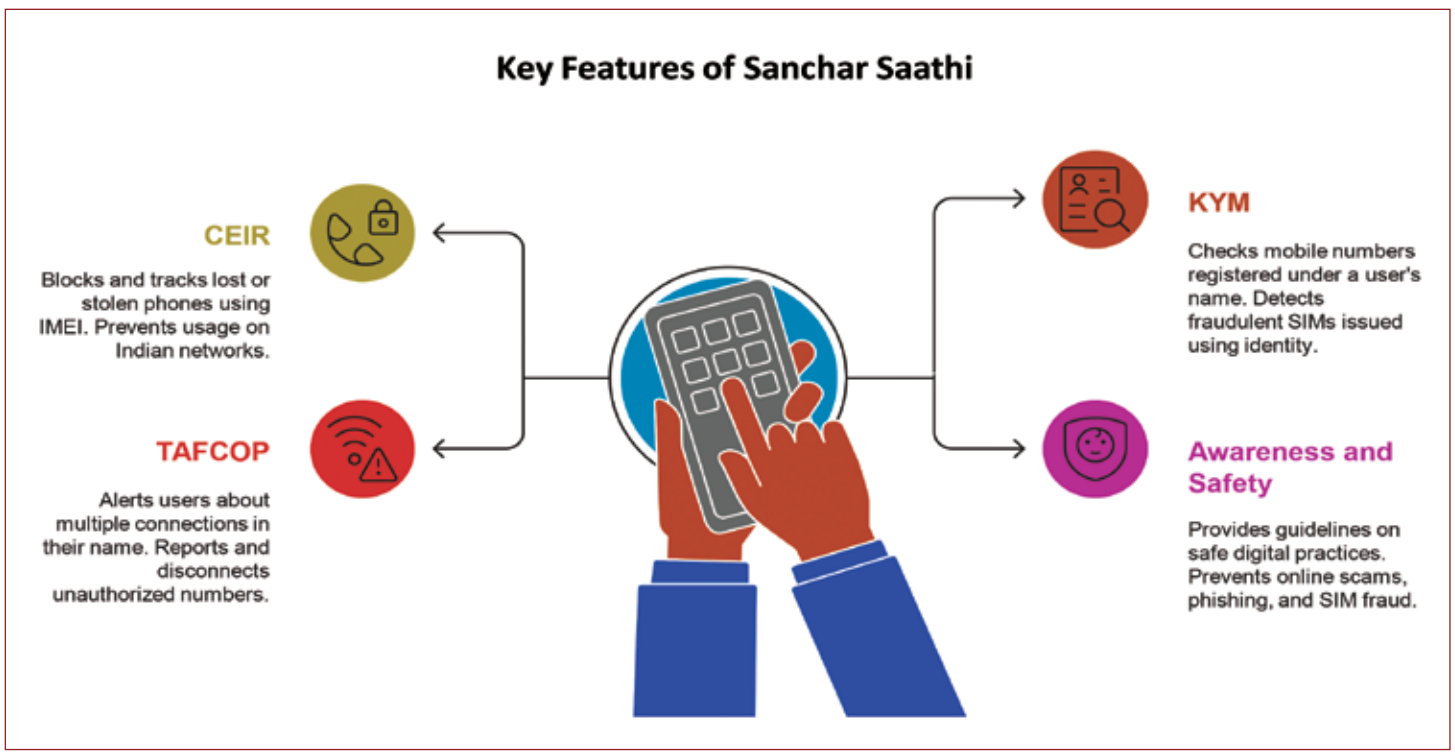
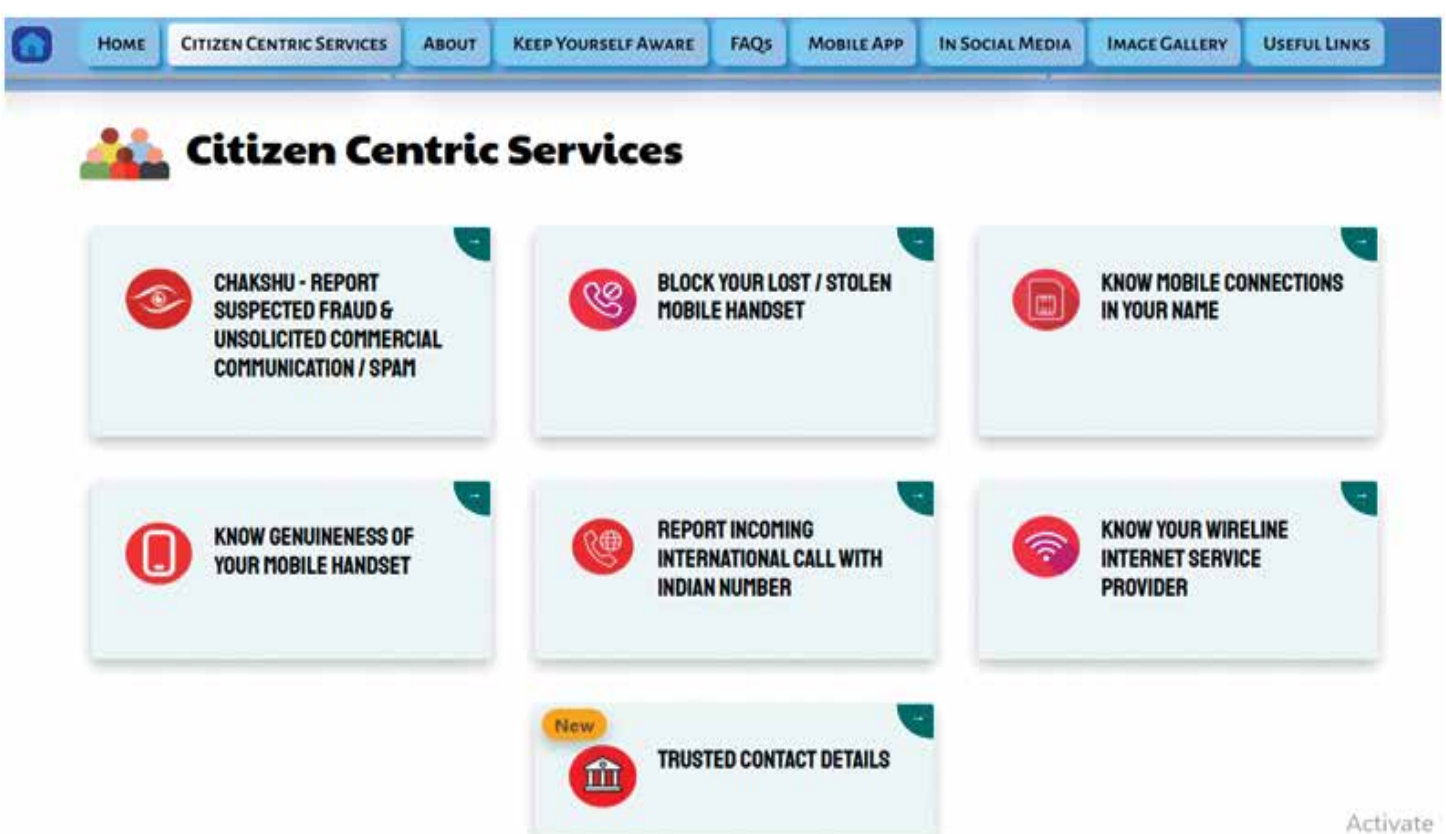


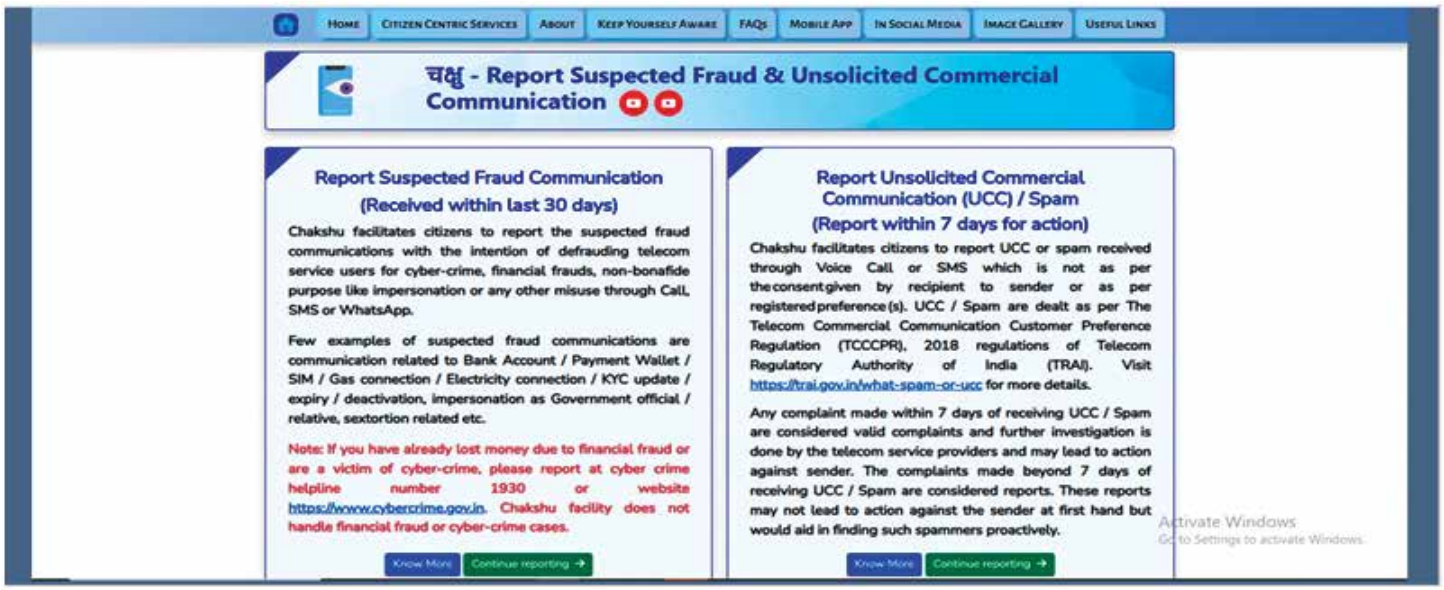

*Figure 4: Key features of Sanchar Saathi*

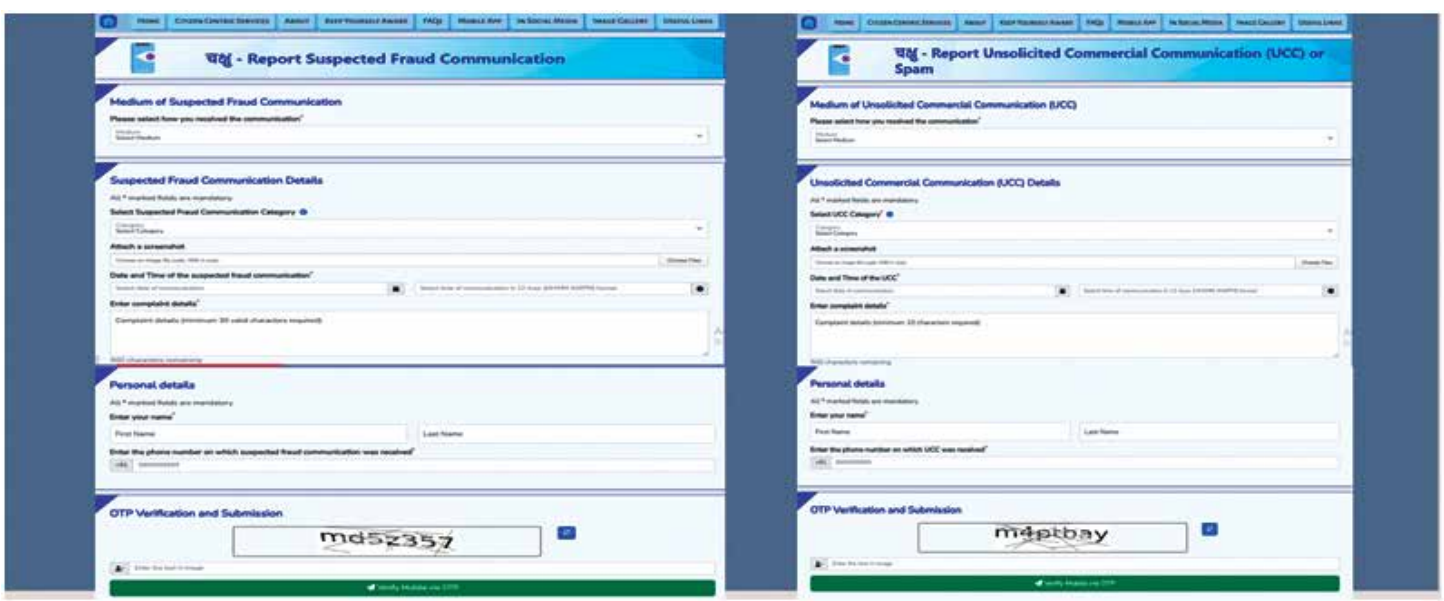
# HOME PAGE VIEW

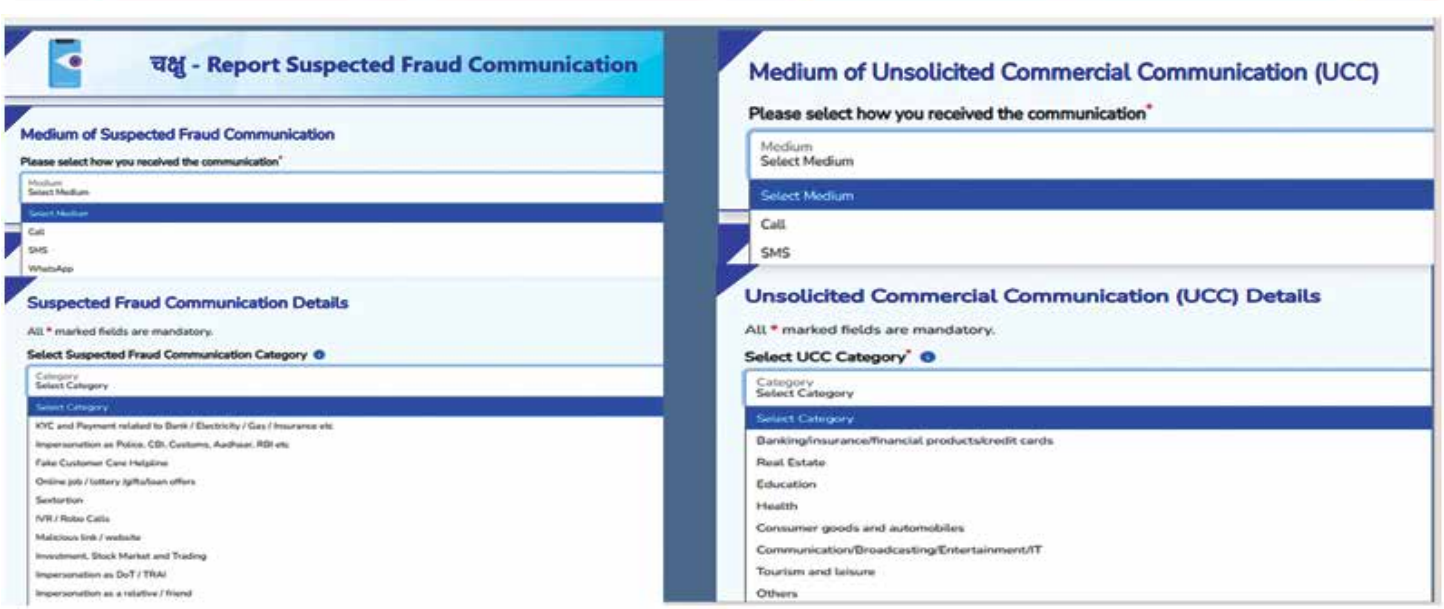
# GO TO CITIZEN CENTRIC SERVICE


# चक्षु–*Report Suspected Fraud & Unsolicited Commercial*




Home
Citizen Centric Services
About
Keep Yourself Aware
FAQs
Mobile App
In Social Media
Image Gallery
Useful Links
चक्षु - Report Suspected Fraud & Unsolicited Commercial Communication
Report Suspected Fraud Communication
(Received within last 30 days)
Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.
Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.
Note: If you have already lost money due to financial fraud or are a victim of cyber-crime, please report at cyber crime helpline number 1930 or website https://www.cybercrime.gov.in. Chakshu facility does not handle financial fraud or cyber-crime cases.
Know More
Continue reporting
Report Unsolicited Commercial Communication (UCC) / Spam
(Report within 7 days for action)
Chakshu facilitates citizens to report UCC or spam received through Voice Call or SMS which is not as per the consent given by recipient to sender or as per registered preference (s). UCC / Spam are dealt as per The Telecom Commercial Communication Customer Preference Regulation (TCCCPR), 2018 regulations of Telecom Regulatory Authority of India (TRAI). Visit https://trai.gov.in/what-spam-or-ucc for more details.
Any complaint made within 7 days of receiving UCC / Spam are considered valid complaints and further investigation is done by the telecom service providers and may lead to action against sender. The complaints made beyond 7 days of receiving UCC / Spam are considered reports. These reports may not lead to action against the sender at first hand but would aid in finding such spammers proactively.
Know More
Continue reporting
Activate Windows
Go to Settings to activate Windows.


चक्षु - Report Suspected Fraud Communication
Medium of Suspected Fraud Communication
Suspected Fraud Communication Details
Personal details
OTP Verification and Submission
md5z357
चक्षु - Report Unsolicited Commercial Communication (UCC) or Spam
Medium of Unsolicited Commercial Communication (UCC)
Unsolicited Commercial Communication (UCC) Details
Personal details
OTP Verification and Submission
m4ptbay


चक्षु - Report Suspected Fraud Communication
Medium of Suspected Fraud Communication
Please select how you received the communication*
Medium
Select Medium
Call
SMS
WhatsApp
Suspected Fraud Communication Details
All * marked fields are mandatory.
Select Suspected Fraud Communication Category
Category
Select Category
KYC and Payment related to Bank / Electricity / Gas / Insurance etc
Impersonation as Police, CBI, Customs, Aadhaar, RBI etc
Fake Customer Care Helpline
Online job / lottery /gifts/loan offers
Sextortion
IVR / Robo Calls
Malicious link / website
Investment, Stock Market and Trading
Impersonation as DoT / TRAI
Impersonation as a relative / friend
Medium of Unsolicited Commercial Communication (UCC)
Please select how you received the communication*
Medium
Select Medium
Call
SMS
Unsolicited Commercial Communication (UCC) Details
All * marked fields are mandatory.
Select UCC Category*
Category
Select Category
Banking/insurance/financial products/credit cards
Real Estate
Education
Health
Consumer goods and automobiles
Communication/Broadcasting/Entertainment/IT
Tourism and leisure
Others

### 2.2.2. NATIONAL CYBER CRIME REPORTING PORTAL (www.cybercrime.gov.in)

The National Cyber Crime Reporting Portal (NCCRP) is a citizen-focused initiative launched by the Ministry of Home Affairs (MHA), Government of India on August 30, 2019under the National Cyber Crime Ecosystem.It provides a centralized online platform to report different types of cybercrimes, especially those targeting women, children, and vulnerable groups.

**Key features of National Cyber Crime Reporting Portal (NCCRP)**

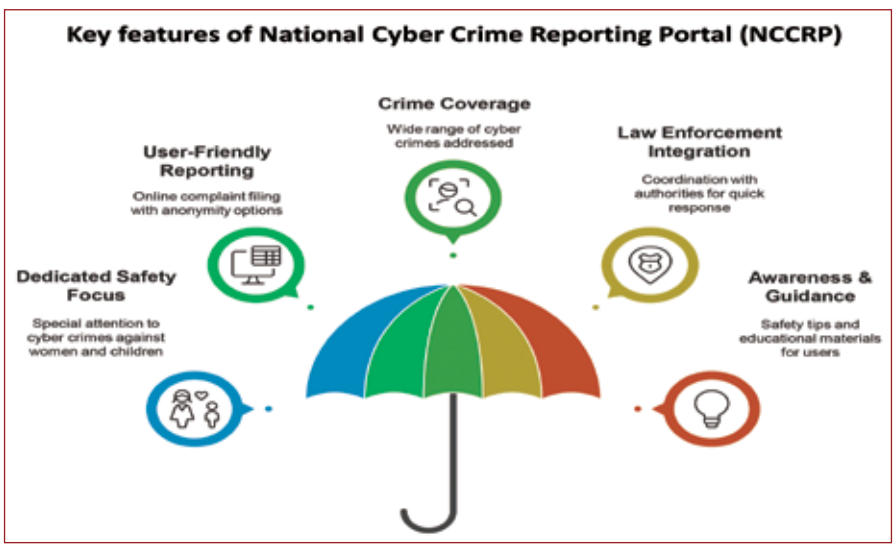
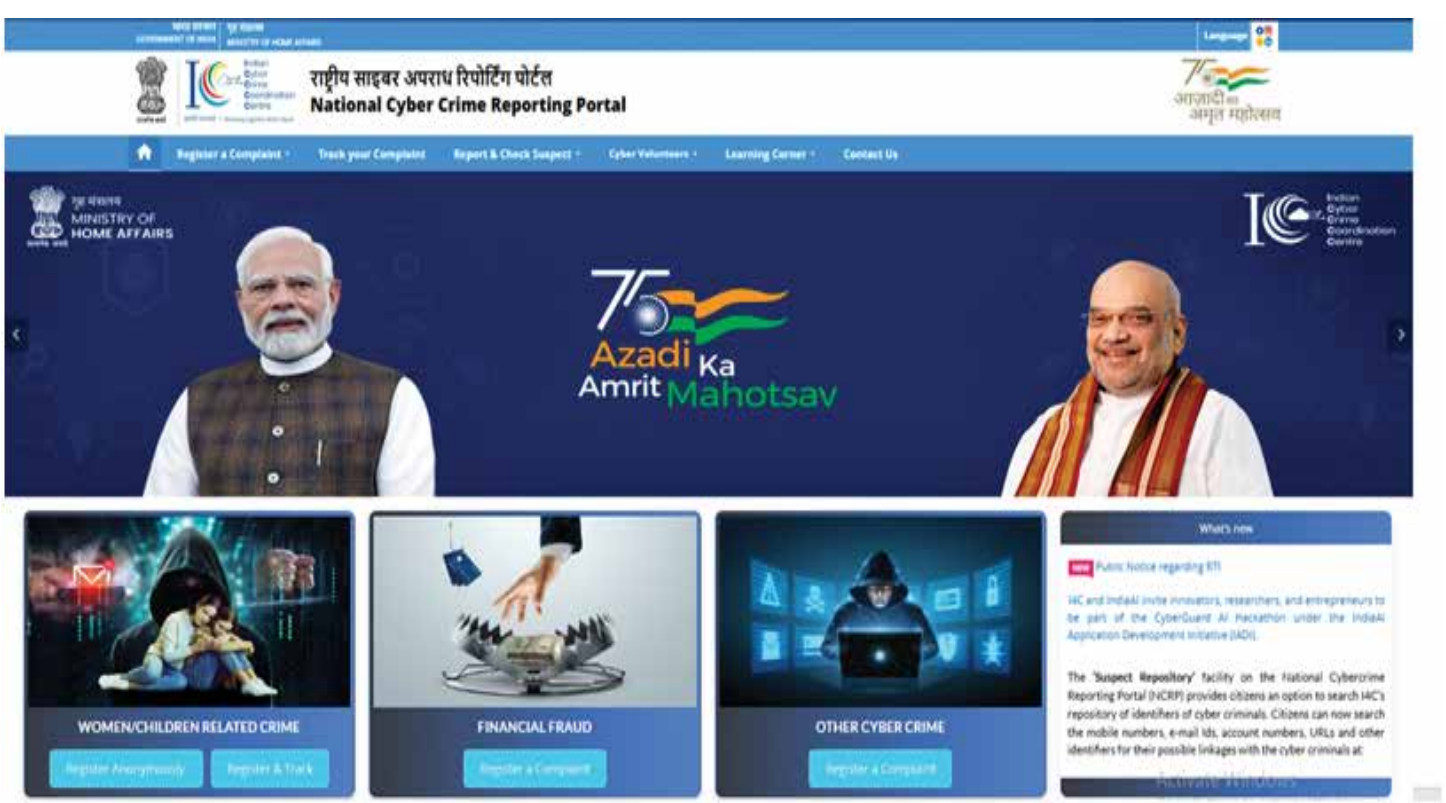
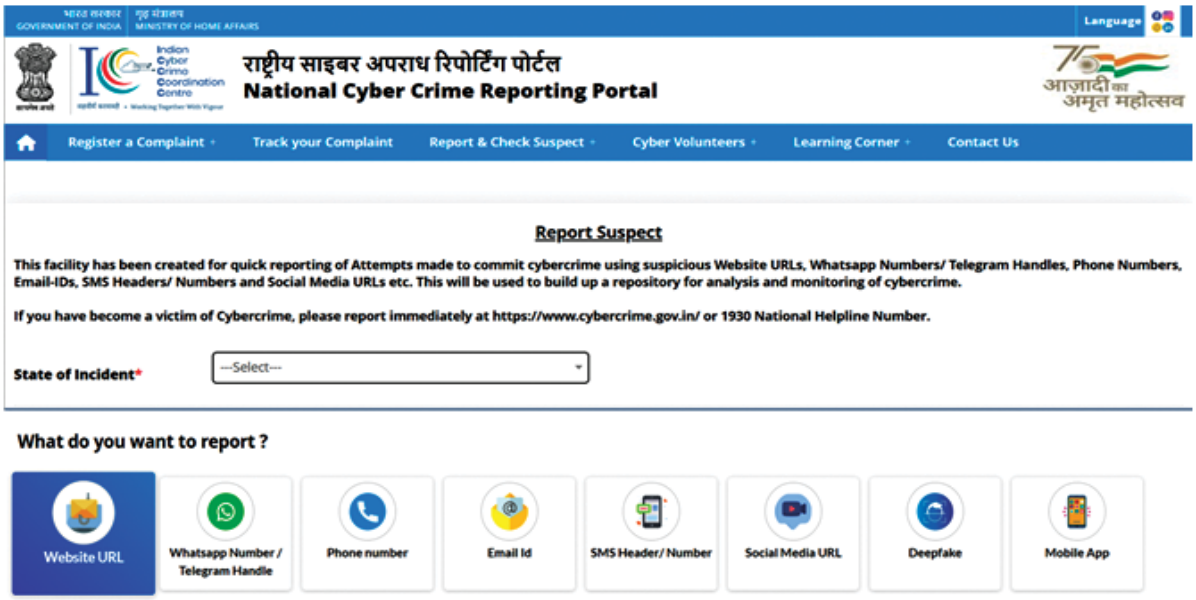



*Figure 5: Key features of NCCRP*

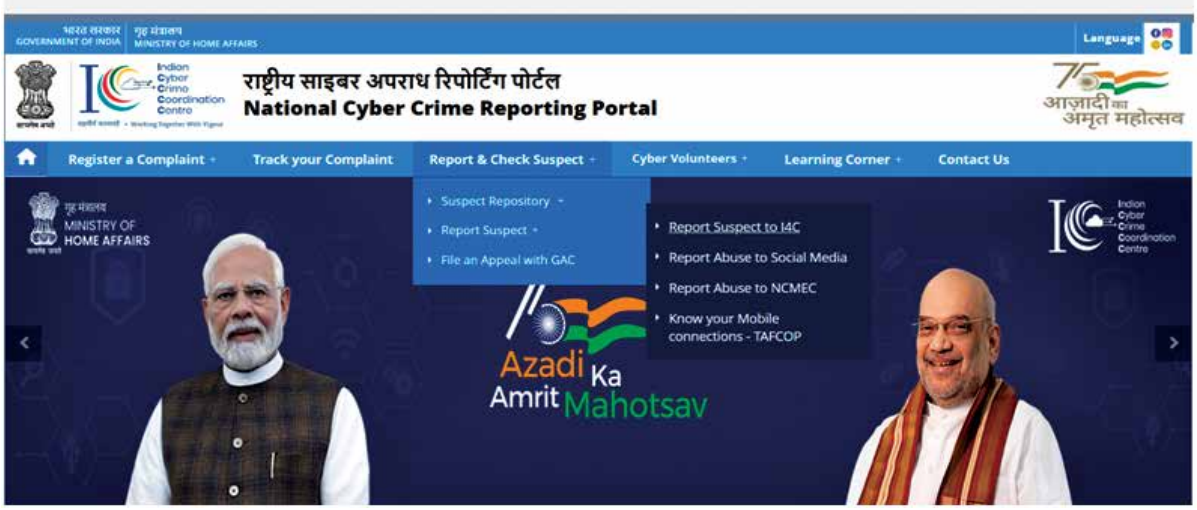
# HOME PAGE VIEW




Report & Check Suspect → Report Suspect → Report Suspect to I4C




## Report & Check Suspect ➡ Report Suspect ➡ Report Abuse to Social Media





# Chapter 3: Protecting the Adolescents from Digital Crime – Literature Review

As India's digital landscape expands rapidly, so does the imperative to protect its most vulnerable populations—children, youth, and women—from online crime. While much of the existing literature details the nature and prevalence of cybercrime, a growing body of research is dedicated to understanding and evaluating the effectiveness of protective measures. This literature review synthesizes key findings on the legal, social, and educational frameworks designed to ensure digital safety in India. It aims to identify effective strategies and research gaps to inform future studies and policy recommendations.

**The legal and policy landscape for digital protection**

The foundation for digital protection in India rests on the Information Technology Act, 2000 (IT Act), which has been crucial in enabling law enforcement to act against online offenses. Academic and legal literature (Sharma & Mishra, 2018) points out that the Act's implementation faces challenges, including low conviction rates and jurisdictional complexities. However, the IT Act, particularly after its 2008 amendment, includes specific provisions against offenses such as cyberstalking, hacking, and publishing of obscene material. In addition to the IT Act, sections of the Indian Penal Code (IPC) related to stalking, defamation, and criminal intimidation are also routinely applied to online crimes. More recent scholarship highlights the increasing role of supplementary legislation, such as the Protection of Children from Sexual Offences (POCSO) Act, in providing specific legal protection against online sexual exploitation of minors. Researchers also note the importance of policy-level initiatives, such as the government's push for digital literacy, in creating a more secure online environment (Jain, 2020).

Beyond legislation, several government programs have been launched to enhance digital safety. The Cybercrime Prevention against Women and Children (CCPWC) Scheme is a notable initiative that funds training for law enforcement and establishes dedicated cybercrime reporting portals. Furthermore, the IndianCyber Crime Coordination Centre (I4C) serves as a national hub for coordinating law enforcement efforts and managing public awareness campaigns. These programs, alongside initiatives like the observance of Cyber Jaagrookta Diwas (Cyber Awareness Day), form a multi-pronged approach to crime prevention and citizen empowerment.

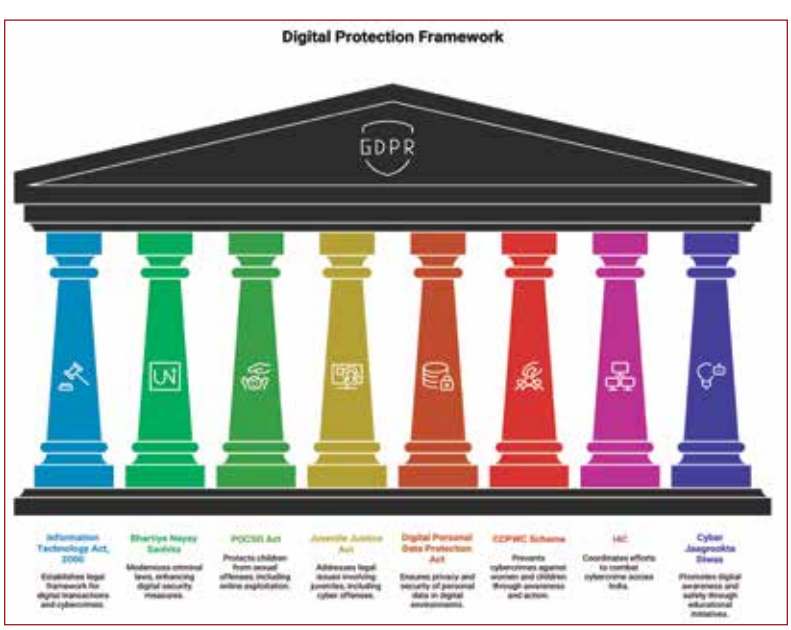



*Figure 6: Digital Protection Framework*

### Adolescents'online risks &behaviors

#### Risk typologies

Key online harms to adolescents include grooming, exposure and distribution of child sexual abuse material (CSAM), cyberbullying, sexual extortion, and exploitation through apps/games (e.g., in-app purchases, predatory contact). These risks are exacerbated by device-level access, encrypted platforms, and lack of parental digital literacy.

#### Online behavior

Adolescents' online behaviors are shaped by media exposure, internet access, and family communication. Schulz et al. (2025) found that violent media exposure and increased internet access predict higher risks of cyberbullying perpetration and victimization, while positive parent–child communication protects against these risks. Zhu (2024) demonstrated that excessive internet use among early adolescents leads to externalizing problem behaviors, mediated by reduced academic expectations and weakened peer relationships, with effects stronger among males and rural youth.

### Threats & Challenges

#### Targeted misinformation & harassment

Adolescents face multiple cyber threats, from harassment and privacy violations to emerging risks like AI-driven manipulation. Nixon (2014) reported widespread prevalence of cyberbullying globally, linking it with depression, anxiety, and psychosomatic symptoms among both victims and perpetrators. Lahti et al. (2024) identified nine types of social media threats, linking them with depression, anxiety, and poor self-rated health. At the global level, the World Economic Forum (2025) warned that generative AI (GenAI) creates new threats, including deepfakes, phishing, and targeted misinformation, requiring systemic policy interventions.

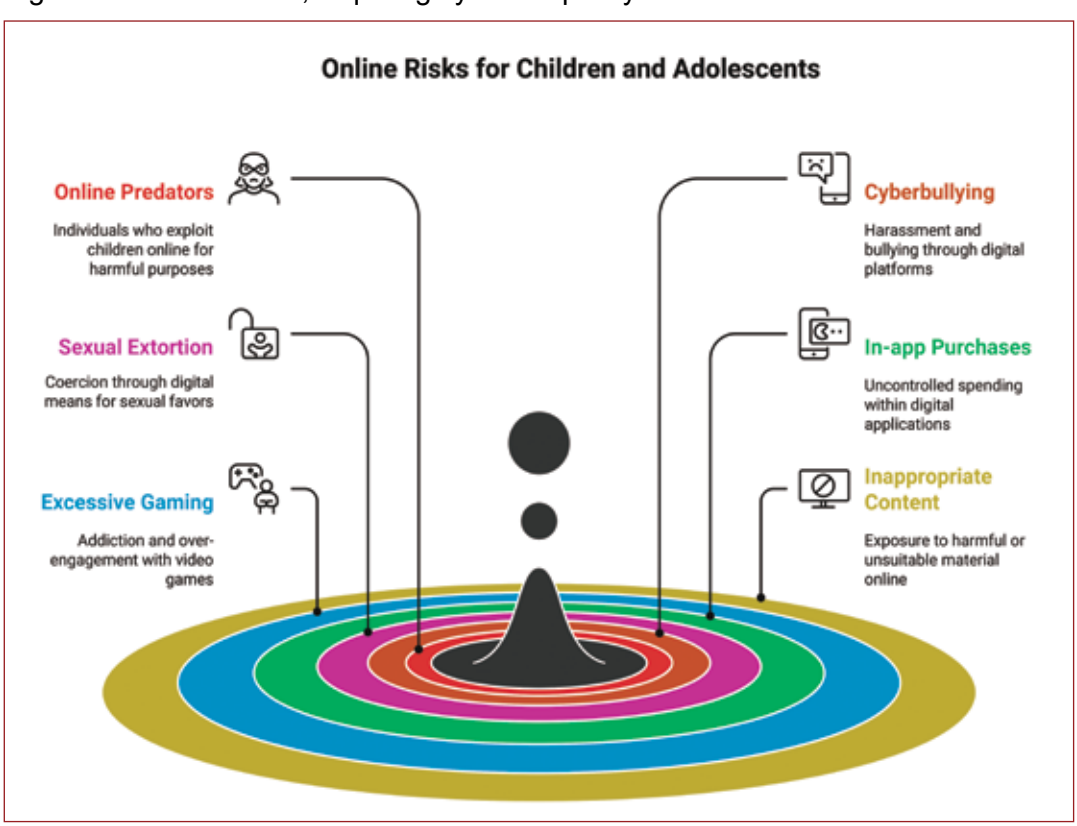



*Figure 7: Online risks to adolescents and children*

**Multi-level strategies for digital safety of adolescents**

**4Cs Risk Framework**

Adolescent cyber safety requires multi-level strategies involving parents, schools, policymakers, and international agencies. Jang (2023) emphasized the importance of the **"4Cs risk framework"—content, contact, conduct, and contract**—in shaping global safety standards. Park et al. (2025) suggested that empowering adolescents is more effective than restrictive parental controls. Similarly, Akter et al. (2025) highlighted that community-driven and multi-stakeholder approaches yield stronger outcomes than family-only.

Innovative interventions have emerged, such as the NettOpp app, which provides psychoeducation and coping strategies for adolescents exposed to cyberbullying (Kaiser et al., 2021). Furthermore, immersive metaverse learning environments have been piloted to reinforce safe practices and awareness of cyber harms (Immersive Metaverse Study, 2025).

**Platform Governance & Safety-by-Design**

Regulators and standards bodies now emphasize "safety-by-design"—platform-level, proactive safeguards alongside transparency and user empowerment (Australian eSafety; OECD, 2024). The UK Online Safety Act (2023) and the Age-Appropriate Design Code (Children's Code) require risk assessments, age assurance, high-privacy defaults, and protections against harmful content for children, shifting duties onto platforms rather than families alone (DSIT/Ofcom guidance; ICO).

**Active & Restrictive Mediation**

Both active (dialogue, co-use) and restrictive (rules/limits) mediation are associated with lower online risks; active mediation also builds digital literacy and positive adaptation (Liu et al., 2023; Ren et al., 2022). Meta-analytic evidence suggests restrictive mediation shows a larger effect on reducing screen time, while active mediation better supports skill-building and resilience—implications point to combining approaches within a whole-family digital ecology. (Liu et al., 2023; Ren et al., 2022).

**Digital Literacy & Online Resilience**

"Resilience" (recognize, recover, and grow from online adversity) is increasingly prioritized over purely restrictive controls. Reviews highlight multi-level models—skills, coping, social support, and platform context—as drivers of adolescents' digital resilience (Rachmayanti et al., 2024; Qamaria et al., 2025). UNICEF's global synthesis balances risks and opportunities and urges embedding resilience within policy, pedagogy, and community practice (Stoilova et al., 2021).

**School-Based, Peer-Led, and Media-Literacy Interventions**

Multiple meta-analyses show school programs reduce cyberbullying perpetration and victimization; effects are modest-to-meaningful and strongest in tailored, whole-school designs (Polanin et al., 2022; Kamaruddin et al., 2023). Peer-education can work but design matters (e.g., peer nomination outperforms volunteers), and media-literacy training improves transferable critical skills (Zambuto et al., 2020; Jeong et al., 2012; Eyal et al., 2024). Technology-enabled interventions (brief video + app messaging) show promise for bystander and coping outcomes (Kutok et al., 2021).

***A study by the Directorate of Education, Delhi (2025), highlighted institutional responses such as cyber safety sessions, digital posters, and assemblies to reduce school-level risks. Similarly, implementation of school safety and security guidelines by NCPCR/NCERT would be a way forward for preventing online crime against adolescents. (The Economic Times, May 2025)***

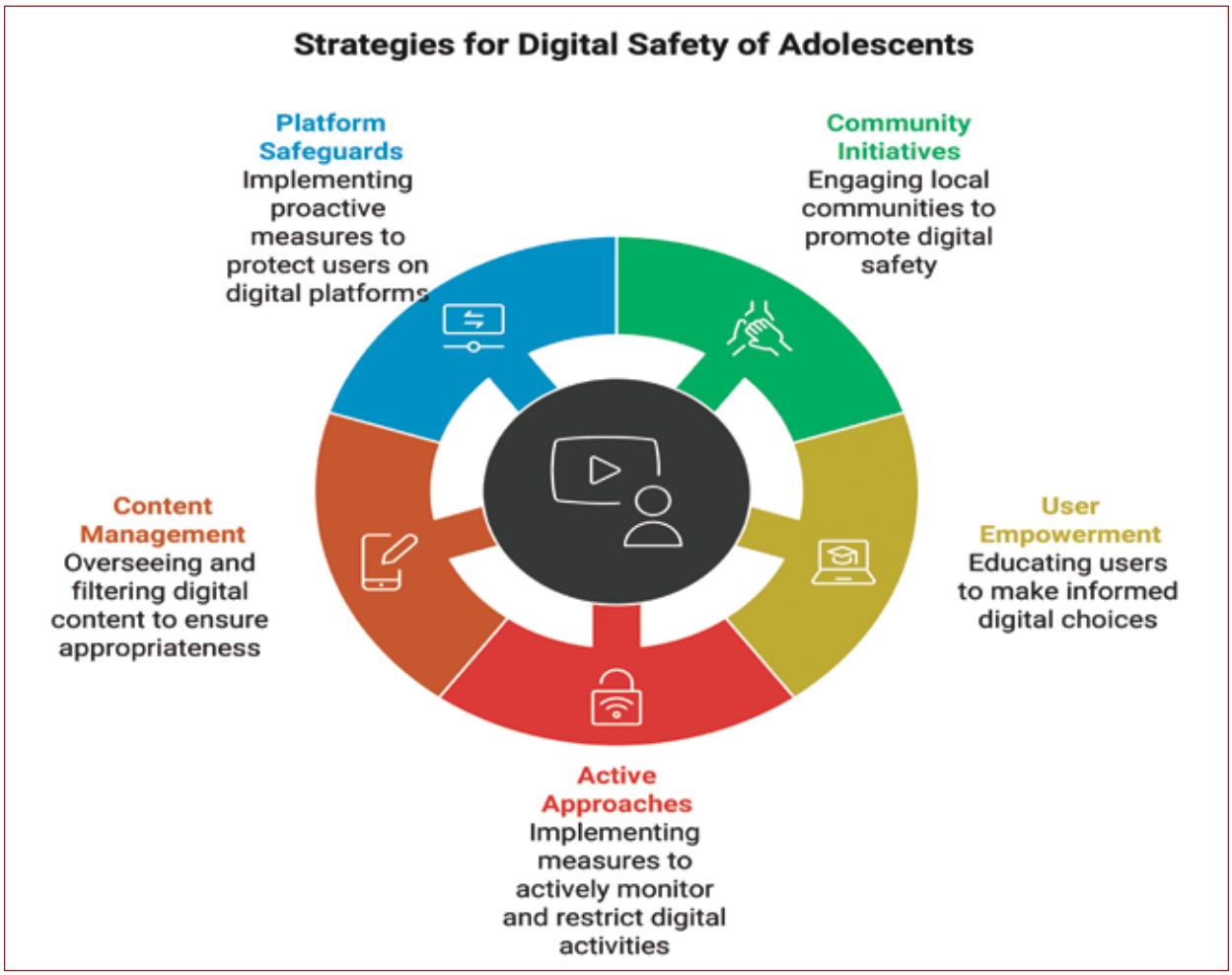



*Figure 8: Strategies for digital safety of adolescents*

**Online digital safety of women**

**Risk typologies**

Women face cyberstalking, publishing private information (doxxing), sexualized harassment, non-consensual image sharing (NCII), image-based abuse including deepfakes, and gendered disinformation/trolling that chills participation in public life. These harms often intersect with offline gender-based violence.

**Threats & Challenges**

Studies on online harassment and trolling highlight the need for greater responsibility from social media platforms. While many platforms have reporting mechanisms, researchers argue that they are often slow or ineffective in addressing the scale of abuse, particularly when it targets marginalized communities (Pal & Sen, 2018).There is a lack of long-term studies that rigorously evaluate the sustained impact of digital safety awareness campaigns on behavior change and the reduction of cybercrime.

More research is needed to assess the effectiveness of training programs for law enforcement officials in handling cybercrime cases, particularly those involving gender-based violence.

**Multi-level strategies for online digital safety of women**

Research indicates that awareness programs focused on empowering women with the knowledge to manage their online presence and recognize threats are highly effective. These groups often provide legal aid and counseling

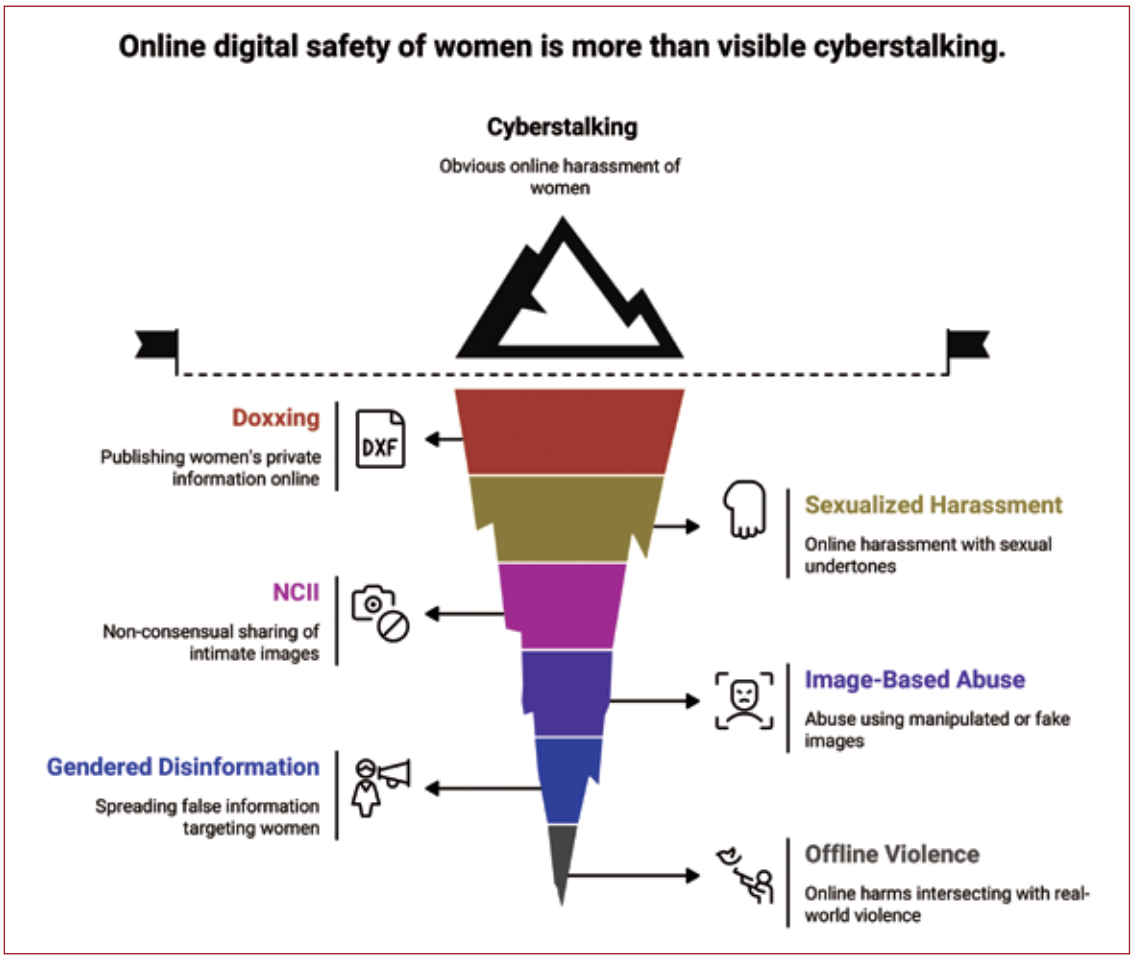



*Figure 9: Cybercrime against women*

services to help women navigate the emotional and practical challenges of online abuse.

Studies on online harassment and trolling highlight the need for greater responsibility from social media platforms. While many platforms have reporting mechanisms, researchers argue that they are often slow or ineffective in addressing the scale of abuse, particularly when it targets marginalized communities (Pal & Sen, 2018).

The literature on cyberstalking and doxing against women (Tiwari, 2021) emphasizes the need for streamlined legal recourse and easily accessible psychological support services. The effectiveness of these measures is often tied to how well they address the unique blend of online and offline intimidation that women face. Research on intersectionality also calls for protective measures that are sensitive to how social hierarchies, such as caste and class, can exacerbate a woman's vulnerability to online harm.

# Chapter 4: About the Study

### 4.1. Rationale for the Study

Being India's capital and a highly linked urban center, Delhi embodies both the advantages and disadvantages of swiftly embracing digital technology. With one of the highest rates of mobile phone and internet penetration in the nation, Delhi's women, youth, and children are all heavily entwined with the digital world. They rely heavily on e-commerce services, social media, ed-tech platforms, financial apps, and smartphones in their daily life.

At the same time, this pervasive connectivity has exposed vulnerable groups to escalating online harms. Children and adolescents face rising digital exploitation, particularly through child sexual abuse material (CSAM), online grooming, and circulation of explicit images. POCSO cases and child cybercrime incidents have been increasing year-on-year, with low conviction rates and delayed redress.

Women and young girls are disproportionately targeted by cyberstalking, sextortion, doxxing, and online harassment. Delhi consistently records a considerable number of crimes against women, with cyber-enabled abuse being a major driver.Youth (13–24 years) are at heightened risk due to heavy engagement on social media, gaming platforms, and digital payments, making them more vulnerable to fraud, impersonation, and online abuse.

While India has enacted robust legal frameworks—the IT Act, 2000; IT Rules, 2021; and the Digital Personal Data Protection Act, 2023—and operationalized national mechanisms like the 1930 cybercrime helpline and the National Cybercrime Reporting Portal, there are scopes of further improvements. These include improving the reporting which is found low due to stigma or lack of awareness, escalating investigation,upscaling conviction rates, limited privacy safeguards for children, and uneven digital literacy among women and marginalized youth.

Therefore, the study is anchored around three interlinked dimensions:

#### 1. Emerging Risks

The OECD (2021) identifies online risks in three broad categories: content risks, contact risks, and conduct risks. In Delhi, these translate into experiences of cyberbullying, trolling, and online harassment; exposure to harmful or extremist content; addictive behaviors linked to gaming and gambling; risks of privacy breaches and identity theft; and gender-specific risks such as stalking and image-based abuse (NCRB, 2023; UNICEF, 2021).

#### 2. Responsibilities

The discourse on children's digital safety emphasizes shared responsibility. Adolescents themselves bear responsibility as active digital citizens, but parents, educators, digital platforms, law enforcement, and policymakers share the duty to create safe and supportive environments. The **UNICEF/ITU "Guidelines for Industry on Child Online Protection"** (2020) stress the role of platforms in implementing robust safeguards, while the National Education Policy (2020) in India highlights digital literacy as a critical competency for schools to impart.

#### 3. Resolutions

Drawing from global practices (e.g., the UK's *Online Safety Bill,* Australia's *eSafety Commissioner*), this study identifies pathways to resolution: establishing multi-stakeholder cyber safety ecosystems, embedding digital literacy in curricula, ensuring gender-sensitive safeguards, empowering adolescents through peer-led initiatives, and advocating for a child-focused regulatory authority in India.

By focusing on Delhi, the study also aims to yield nationally scalable lessons on strengthening cyber safety frameworks, designing genderand age-sensitive digital literacy programs, and building an inclusive, safe and accountable institutions and digital platforms.

### 4.2. Objectives of the Study

The primary objective of this study was to examine the perspectives of adolescents, parents, school authorities, CWCS and Police officials on issues of cyber safety in Delhi. Specifically, the study aimed to:

1. To map digital access and usage patterns among adolescents in Delhi, highlighting opportunities and vulnerabilities.
2. To analyze the nature and prevalence of emerging risks encountered by adolescents online.
3. To examine the roles and responsibilities of adolescents, families, educators, digital platforms, and policymakers in addressing online risks.
4. To recommend actionable and context-specific resolutions that can strengthen adolescent online safety in Delhi while aligning with national and global child protection frameworks.

### 4.3. Research Questions

The study was guided by the following research questions:

**1. Adolescents' Digital Access and Practices**

- What is the level of access to digital devices and the internet among adolescents?
- How do adolescents use digital platforms, and what are their awareness levels and practices regarding cyber safety?

**2. Parental Perceptions and Monitoring**

- How do parents perceive cyber safety risks for their children?
- What monitoring practices, strategies, and challenges do parents face in guiding adolescents' online behavior?

**3. School Authorities' Preparedness**

- What policies, mechanisms, and initiatives have schools adopted to promote cyber safety among adolescents?
- How effectively are these policies implemented at the institutional level?

**4. Institutional Roles (CWCs and Cyber Police)**

- What roles do Child Welfare Committees (CWCs) and the Cyber Police play in preventing and addressing cyber-related risks among adolescents?
- What challenges do these institutions face in enforcing cyber laws and providing protection to children online?

**5. Risks, Vulnerabilities, and Coping Mechanisms**

- What are the key risks and vulnerabilities adolescents face in cyberspace?
- How do adolescents, families, and schools cope with these challenges?

6. **Recommendations and Way Forward**

- What evidence-based interventions can strengthen cyber safety education and awareness at the school, family, and community levels?
- How can different stakeholders—adolescents, parents, schools, CWCs, police, and NGOs—collaborate to create a safer digital environment?

### 4.4. Scope of the study

The scope of this study was designed to ensure a comprehensive and multi-dimensional exploration of cyber safety among adolescents. The following aspects define its boundaries and coverage:

1. **Stakeholder Coverage**

   The study engages three primary stakeholder groups—adolescents, parents, school authorities, child welfare committee (CWC), and police—to capture diverse perspectives on digital access, risks, and protective mechanisms.This multi-level approach enables triangulation of findings, ensuring that the issue is understood from the point of view of users (adolescents), caregivers (parents), and institutions (schools).

2. **Mixed-Methods Approach**

   The study uses quantitative surveys with adolescents and parents to generate measurable data on access, practices, and awareness.It also incorporates qualitative insights through Key Informant Interviews (KIIs) with school authorities CWCs and Police, adding depth and contextual understanding.This combination strengthens both statistical validity and narrative richness of the findings.

3. **Geographic Representation**

   The study was conducted across six districts of Delhi: South East, North West, West, Central, North East, and South.Equal representation of respondents from each district ensures geographical balance and comparability across regions.Although Delhi is an urban setting, intra-city variations in school types, socio-economic backgrounds, and digital exposure provide a diverse urban sample.

4. **Application of Findings**

   The findings are intended to guide policy issues, especially in assisting the implementation of cyber safety policies in schools and integrating cyber safety education in curricula.Evidence from the study is also meant to inform school-based interventions, including structured awareness programs, teacher training, and reporting mechanisms.

   For parents, the study highlights gaps in monitoring and communication, aiming to support awareness campaigns and capacity-building initiatives at the household level.More broadly, the insights contribute to shaping community-level discourse on adolescent online safety, with potential linkages to state and national policy frameworks.

### 4.5. Limitations of the Study

Despite its robust design, the study faced certain methodological and contextual limitations which must be acknowledged:

1. **Geographical Constraints**

   The research is geographically confined to six districts of Delhi, an urban metropolitan area.While findings are relevant to similar urban contexts, they may not fully reflect realities in rural areas or smaller towns, where digital penetration, parental awareness, and institutional preparedness differ significantly.

2. **Reliance on Self-Reported Data**

Data on sensitive issues such as cyberbullying, online harassment, or sharing of personal information was self-reported by adolescents and parents.Such responses may be influenced by underreporting, recall errors, or social desirability bias, thereby underestimating the true extent of risks.

3. **Cross-Sectional Design**

The study is cross-sectional, capturing responses at a single point in time.It cannot track long-term behavioral changes, evolving digital trends, or the impact of interventions over time.A longitudinal design would have provided stronger evidence of causal relationships and trends.

4. **Representation Gaps**

The majority of schools covered were government institutions (89%), with limited representation from private schools.Similarly, among parents, mothers formed the majority (69%), leading to underrepresentation of fathers or male caregivers.These gaps may affect the generalizability of findings across all institutional types and household dynamics.

5. **Contextual Factors**

Broader legal, institutional, and cultural dimensions—such as the role of Child Welfare Committees (CWCs), the Police, or variations in state-level implementation of cyber laws—were only partially explored.As such, while the study provides valuable micro-level insights, it is less comprehensive on systemic and enforcement-related aspects of cyber safety.

# Chapter 5: Study Design

## 5.1. Study Methods

The study employed a mixed-methods design, integrating both quantitative and qualitative approaches to ensure comprehensive coverage of the research objectives. Quantitative surveys with adolescents, parents and school authorities provided measurable data on digital access, practices, and awareness, while qualitative methods – Key Informant Interviews (KIIs) – CWCs and Police officials allowed for deeper exploration of perceptions, institutional practices, and contextual realities. This combination facilitated both **breadth (statistical representation) and depth (contextual insights)** of analysis.

## 5.2. Study Area and Population

5.2.1. **Study Area:** The research was conducted in six districts of Delhi—South East, North West, West, Central, North East, and South. These districts were purposively selected to ensure geographical representation and comparability across diverse socio-economic contexts.

### 5.2.2. Study Population:

1. **Adolescents:** Students aged 10–19 years enrolled in government and selected private schools.
2. **Parents/Guardians:** Caregivers of the adolescents, representing both mothers and fathers.
3. **School Authorities:** Principals, teachers, and IT staff responsible for student learning, digital education, and welfare.

## 5.3. Sampling Strategy and Sample Size

5.3.1. **Sampling Strategy:** A stratified purposive sampling method was used to ensure proportional representation across districts and a balanced gender ratio among adolescent respondents.

5.3.2. **Sample Size:** Adolescents: A total of 4800 respondents were surveyed, with 800 adolescents drawn from each of the six districts. The sample was deliberately balanced to ensure equal representation of boys and girls (50% each), thereby minimizing gender bias and enabling comparative analysis.

5.3.3. **Parents/Guardians:** A total of 1200 parents/guardians (male and female equally) participated in the study. The sample was equally distributed across two age groups—below 30 years and above 30 years (50% each). Both mothers and fathers were proportionately included; however, mothers demonstrated higher responsiveness and participation rates.

5.3.4. **School Authorities:** From each of the six districts, three school representatives (teachers and/or principals) were selected, resulting in a total of 18 respondents. The sample primarily consisted of government school representatives, with selective inclusion of private schools to reflect institutional diversity and capture variations in policies and practices.

## 5.4. Data Collection Methods

### 5.4.1. Quantitative Survey

Structured questionnaires were administered to adolescents, parents and school authorities. The survey captured demographic details, internet access, device ownership, online behavior, awareness of cyber safety, and experiences of online risks.

#### 5.4.2. Key Informant Interviews (KIIs)

KIIs were undertaken with CWC members, CWC chairperson and Police officials. These interviews explored institutional responses, policy-level practices, and challenges in promoting cyber safety.

#### 5.4.3. Data Collection Tools

- **Questionnaires:** Structured tools with both closed-ended and open-ended questions for adolescents and parents.
- **FGD Guides:** Semi-structured guides tailored to adolescents and parents, ensuring participatory and age-sensitive engagement.
- **KII Checklists:** Interview frameworks for school authorities and stakeholders, designed to elicit institutional perspectives and best practices.

All tools were **pre-tested and refined** for clarity, cultural sensitivity, and age appropriateness before full-scale administration.

### 5.5. Data Analysis Procedures

#### 5.5.1. Quantitative Data Analysis

- Data were entered, cleaned, and organized in Microsoft Excel.
- Analysis involved descriptive statistics (frequency, percentage, mean) and cross-tabulations to examine relationships between demographic variables (e.g., age, gender, school type) and cyber safety awareness/practices.
- Findings were presented in tables and charts for clarity and accessibility.

#### 5.5.2. Qualitative Data Analysis

- Transcripts from FGDs and KIIs were coded thematically using pre-identified categories (e.g., access, awareness, risks, parental monitoring, institutional mechanisms).
- Emerging themes were further synthesized into patterns that complemented quantitative findings.
- Direct quotes and narratives were integrated to provide contextual richness and highlight participant voices.

### 5.6. Ethical Considerations

- **Informed Consent:** All participants provided voluntary consent; parental consent was obtained for adolescents below 18 years.
- **Confidentiality:** Anonymity of respondents was maintained, with no personally identifiable information disclosed.
- **Voluntary Participation:** Respondents were informed of their right to withdraw at any stage without consequences.
- **Sensitive Topics:** Issues such as cyberbullying and online exploitation were handled with sensitivity. Referral information for counseling and support services was provided where needed.

### 5.7. Limitations of the Methodology

Despite careful design, the study faced certain methodological constraints:

1. **Self-Reported Data:** Reliance on self-reported information may have led to underreporting of sensitive experiences (e.g., cyberbullying, online exploitation) due to fear, stigma, or social desirability bias.
2. **Representation Gaps:** Private schools and male caregivers were underrepresented, limiting the comparability of findings across all institutional and parental contexts.
3. **Qualitative Depth:** The number of FGDs and KIIs was restricted due to time and logistical constraints, potentially limiting the depth of qualitative insights.
4. **Cross-Sectional Design:** The study provides a snapshot in time, which does not allow for examination of long-term behavioral changes or the evolving nature of digital risks.

# Chapter 6: Conceptual Framework&Definitions

### 6.1. Ecological Systems Theory: A Combined Framework

This model integrates Ecological Systems Theory with the principles of the UNCRC and Digital Citizenship to provide a comprehensive, multi-layered framework for addressing online safety. It argues that ensuring a child's or individual's rights and fostering their responsible behaviour is not just an individual task, but a collective effort involving all levels of their environment.

- **Microsystem (Individual & Immediate Environment):** At this level, the focus is on the individual's direct interactions. Digital Citizenship principles (like Digital Literacy and Digital Etiquette) are crucial here. These are the skills and behaviours that an individual, and those immediately around them (like family and friends), can directly control. The goal is to empower the user to be a confident and safe online citizen.
- **Mesosystem (Interactions between Environments):** This level focuses on the connections between a person's different microsystems. For example, how a parent's digital safety rules at home (microsystem 1) are reinforced by a teacher's digital literacy curriculum at school (microsystem 2). The framework suggests that the UNCRC's approach must be upheld across these systems. For instance, a child's right to privacy must be respected by parents, schools, and their peer group.
- **Exosystem (External Systems that Impact the Individual):** This level includes systems that indirectly affect the individual but in which they don't have a direct role. This is where the UNCRC becomes a powerful advocacy tool. The **right to protection** (Article 19) places a responsibility on technology companies and governments (part of the exosystem) to create safe digital environments. This includes designing platforms with strong privacy settings and effective reporting mechanisms, which then influence the user's direct experience in the microsystem.
- **Macrosystem (Societal & Cultural Norms):** This is the broadest level, encompassing cultural values and laws. This is where the UNCRC's principles of **non-discrimination** and the **best interests of the child** become the guiding light. The macrosystem determines whether society values children's online safety and whether laws are in place to hold tech companies and governments accountable for upholding children's rights.
- **Chronosystem (Change over Time):** This dimension highlights how all of these systems and their interactions change over an individual's life. As children grow and their "evolving capacities" mature (a UNCRC concept), their needs for online safety and their digital citizenship skills evolve. A framework that combines these theories can dynamically adapt to these changes, from providing basic supervision for a young child to fostering advanced critical thinking and advocacy skills in a teenager.

This combined framework provides a holistic view, moving beyond just teaching skills (Digital Citizenship) or asserting rights (UNCRC) to considering the entire ecosystem that either supports or hinders a safe and rights-respecting digital experience.

### 6.2. Key Concepts and Definitions

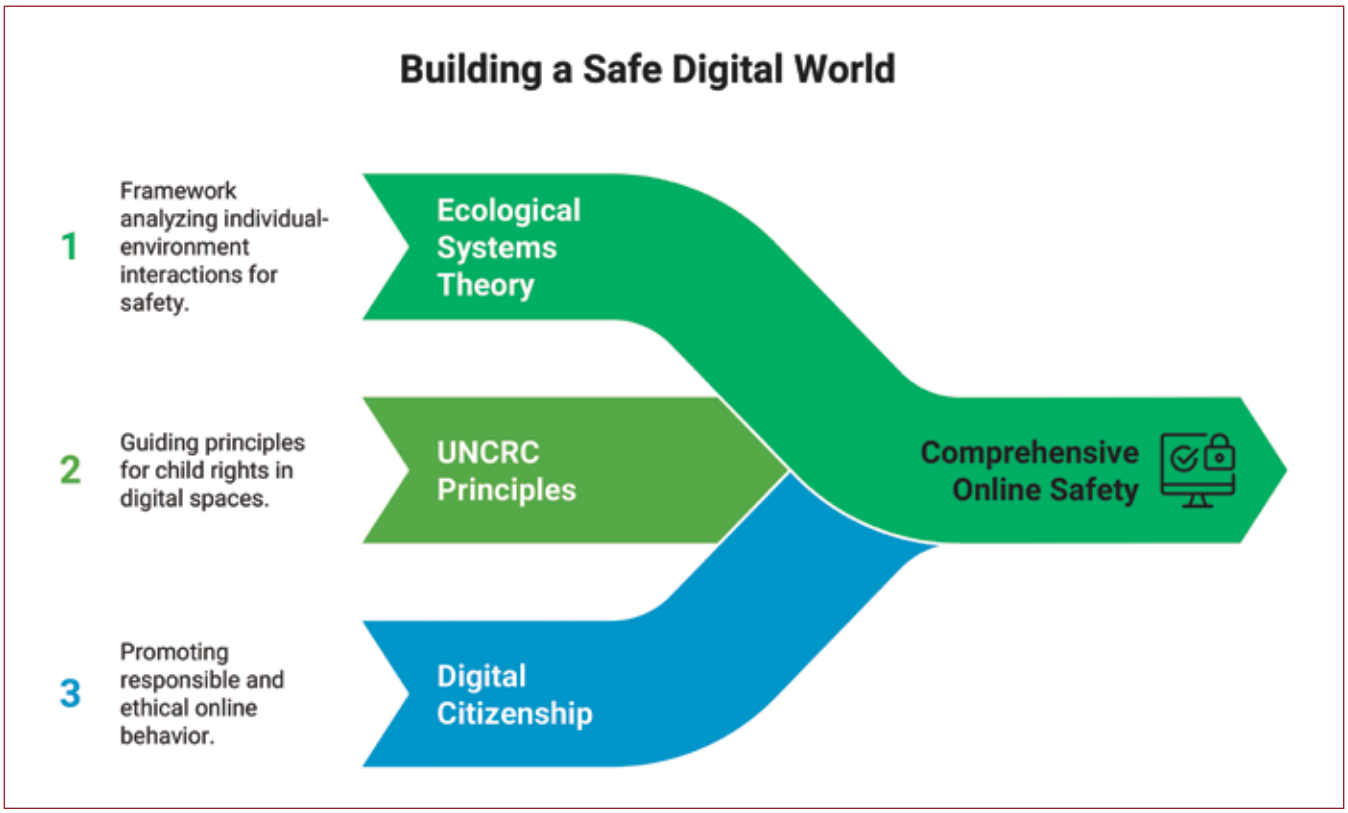



*Figure 10: A Combined Framework for Online Safety of Children*

**Online Digital Safety**

Protecting people from online dangers like cyberbullying, exploitation, fraud, misinformation, and privacy violations, especially for vulnerable populations like women, children, and young people. It covers legal protections, digital literacy, and technical precautions.

**Cyberbullying**

Harassment, humiliation, or intimidation conducted via digital platforms (social media, messaging apps, gaming platforms).

- **Children/Youth:** Peer-based bullying, body shaming, trolling.
- **Women:** Gendered abuse, sexual harassment, doxxing.

**Online Child Sexual Exploitation and Abuse (OCSEA)**

The use of digital platforms to exploit or abuse children sexually (grooming, image-based abuse, sextortion, trafficking).

**Cyberstalking & Online Harassment**

Persistent unwanted digital surveillance, threats, or harassment.

- **Women** are disproportionately targeted.
- Includes revenge porn, unsolicited explicit messages, and impersonation.

**Data Privacy & Protection**

The safeguarding of private information (such as names, addresses, locations, Aadhaar numbers, etc.) against abuse, illegal access, or profiling. It is essential for women/youth utilizing social media and children using ed-tech platforms.

**Digital Literacy / Digital Citizenship**

The knowledge, skills, and values enabling safe, responsible, and ethical participation online. It includes critical thinking, privacy awareness, consent, and respectful engagement.

**Misinformation & Disinformation**

- Misinformation: False information spread without intent to harm.
- Disinformation: False or manipulated information spread deliberately.

Risks for youth (radicalization, fake news) and women (gender stereotypes, misinformation around health/rights).

**Online Gender-Based Violence (OGBV)**

Any harmful act directed at an individual based on their gender that is carried out online. It includes cyberflashing, hate speech, slut-shaming, and deepfakes.

**Phishing, Hacking & Financial Fraud**

Digital crimes where individuals are tricked into sharing sensitive information (bank details, OTPs, UPI pins).

- **Youths:** Targeted through gaming or crypto scams.
- **Women:** Targeted with fake job/loan offers or identity theft.

**Digital Well-being**

Balancing technology uses to promote mental health, reduce addiction, and prevent harmful impacts of excessive screen time.

**Digital Resilience**

The capacity of individuals—especially vulnerable populations—to recover from online harms, adapt to challenges, and make informed choices.

*Table 1: Online Digital Safety Matrix*

| Online Digital Safety Matrix: Children, Youth, and Women | | | |
|---|---|---|---|
| **Concept** | **Children** | **Youth** | **Women** |
| **Cyberbullying** | Online class bullying, body shaming, exclusion from peer groups | Trolling, cancel culture, hate speech in peer networks | Gendered abuse, misogynistic trolling, professional defamation |
| **Protections** | Parental mediation, school cyber-safety policies, POCSO | Digital literacy programs, peer support networks | Cybercrime cells, anti-harassment laws, reporting mechanisms |
| **Online Child Sexual Exploitation & Abuse (OCSEA)** | Grooming, sextortion, circulation of CSAM | Exploitation via dating apps, sextortion scams | Image-based sexual abuse, revenge porn |

| | | | |
|---|---|---|---|
| **Protections** | POCSO Act, awareness campaigns, reporting hotlines (NCPCR, Cybercrime portal) | IT Act provisions, digital resilience programs | IT Rules 2021, legal recourse, platform takedowns |
| **Cyberstalking & Harassment** | Stranger danger on gaming/ social platforms | Stalking via social media, fake accounts | Persistent harassment, cyberstalking, deepfakes |
| **Protections** | Restricted app use, parental control, awareness drives | Cyber laws (BNS/IT Act), campus sensitization | Cybercrime helplines, gender-sensitive policing |
| **Data Privacy & Protection** | Ed-tech apps collecting personal data | Oversharing on social media, data theft in startups/gigs | Financial data breaches, doxxing, Aadhaar/ID leaks |
| **Protections** | DPDP Act compliance for child data | Youth awareness on consent/data | Stronger privacy laws, digital hygiene campaigns |
| **Digital Literacy / Citizenship** | Need for age-appropriate digital safety curriculum | Critical thinking against misinformation, scams | Safe use of professional/ social platforms, reporting OGBV |
| **Protections** | NCERT/CBSE cyber safety curriculum, parental guidance | University/college campaigns, peer digital ambassadors | NGOs, awareness campaigns, Women's safe digital spaces |
| **Misinformation / Disinformation** | Fake educational/health info (e.g., COVID myths) | Political/religious radicalization via disinformation | Health misinformation, gender stereotypes |
| **Protections** | Child-friendly fact-check initiatives | Media literacy modules in higher education | Fact-check platforms, awareness drives |
| **Online Gender-Based Violence (OGBV)** | Early exposure to gendered abuse, gaming insults | Online dating violence, sexual harassment | Cyberflashing, hate speech, slut-shaming |
| **Protections** | Awareness programs in schools | Campus-level redress systems, IT Act provisions | Helplines, fast-track cyber courts, platform safety tools |
| **Phishing, Hacking & Financial Fraud** | Gaming app scams, phishing links in cartoons/games | Crypto scams, loan apps, phishing via social media | Fake job offers, financial scams, identity theft |
| **Protections** | Parental monitoring, digital hygiene lessons | Financial literacy, awareness campaigns | Banking security protocols, RBI grievance systems |
| **Digital Well-being** | Screen-time addiction, sleep disruption | FOMO, mental health issues from online pressure | Stress from harassment, work-life digital imbalance |
| **Protections** | Parental guidance, wellness programs | Counselling, youth mental health helplines | Gender-sensitive wellness resources, safe reporting |
| **Digital Resilience** | Building coping skills, safe reporting behaviour | Peer-based resilience networks | Empowerment through awareness, survivor networks |
| **Protections** | School programs, guidelines | Youth NGOs, resilience-building modules | Women's collectives, online self-defence trainings |

# Chapter 7: Key Findings from the Study

The key findings provide empirical insights into adolescents' digital practices, emerging risks, and resolutions based on the discussion with adolescents, themselves, parents, school authorities, child welfare committees and cyber police.

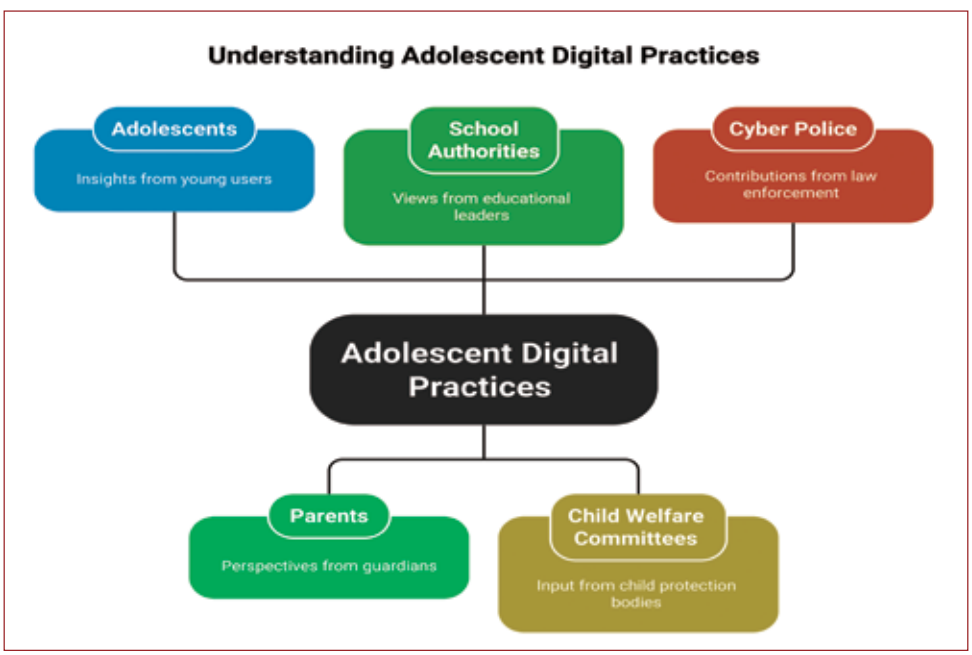



*Figure 11: Adolescents digital practices*

## 1. Adolescents

### Access to internet and devices

- A very high proportion of adolescents (83.6%) reported having internet access at home, reflecting deep digital penetration.Two-thirds (65.4%) own a personal device, while the remaining depend on parents' or siblings' devices.
- Smartphones dominate (97%) internet access, while computers, tablets, and smart TVs account for less than 3%. This reflects affordability, convenience, and peer-driven usage trends.

### Digital engagement patterns

- 41% spend 1–2 hours online daily, while one-fourth (25%) spend 3–4 hours. However, nearly 14% engage for over 4 hours, signaling risks of overexposure and possible digital addiction.
- Social media is highly prevalent: 61% of adolescents own social media accounts, while 39% rely on parental or siblings' accounts.
- 35% maintain multiple accounts on the same platform, mainly for entertainment (44%), privacy/safety (6%), or popularity (6%). This indicates experimentation with multiple identities and varied motivations in the online space.

**Awareness and practices**

- Awareness of the term “cyber safety” is very high (84%), with schools playing a leading role (28%), followed by parents, media, and friends.
- Commonly recognized safe behaviors include **not sharing passwords** (29%), avoiding strangers (18%), and identifying fake news (13%).

**Unsafe behaviors persist**

- 32% admit to sharing personal information online.
- 41% sometimes or always accept friend requests from strangers.
- 45% never change passwords; only 15% change monthly.
- 40% do not use privacy settings, and 14% are unaware of them.

**Experience of online risks**

- While **54% report no online risks**, significant proportions experienced:
  - Cyberbullying (12%)
  - Pressure to share personal media (10%)
  - Scams or fraud (6%)
  - Account hacking/theft (3%)
  - Inappropriate content (2%)

**Attitudes and confidence**

- **70% consider cyber safety a very serious issue**, reflecting strong recognition of risks.
- Confidence in navigating the internet is relatively high (68%), yet one-third of adolescents remain unsure or lack confidence, pointing to the **need for continuous digital literacy support.**

**2. Parents**

- **77% parents were between 21 - 40 years**, which suggests higher digital familiarity compared to older generations.
- Mothers dominate participation (69%), reflecting their caregiving roles and availability at home.
- 54% parents studied up to 10th or below, while 21% attained higher education, highlighting **uneven capacity for digital literacy.**

**Children’s internet use**

- **93% of children have internet access;** 51% use personal devices, indicating high independence.47% spend 1–3 hours daily, 26% spend more than 4 hours, raising risks of addiction and reduced offline activities.

**Children’s lifestyle**

- Parents observe **negative lifestyle changes:**
  - 47% reported sleep disorders.

- 46% noticed changes in food behavior, often linked to screen use and exposure to unhealthy advertisements.

**Awareness and supervision**

- **69% parents** informed that their children are aware of cyber safety.
- **Parental supervision:**
  - 39% supervised children's online activities regularly.
  - 30% rarely monitor.
  - 11% never monitor at all.
- **Understanding of parental control tools in social media applications:** 58% do not understand them while 22% are unaware that such features exist.
- **Parent-child communication is inconsistent:** 32% rarely discuss cyber safety, and 14% never do. This lack of dialogue may prevent children from confiding in parents about risks.

**Perceptions of threats to their children**

- Parents identify key threats:
  - Phone addiction and excessive screen use (23%).
  - Social media risks like fake identities, unsafe platforms (20%).
  - Online scams/frauds (16%).
  - Privacy and data security (11%).
- Interestingly, 18% reported "no threats," possibly reflecting **underestimation of risks** or overconfidence in parental supervision.

**Expectations from schools**

- Parents strongly expect schools to play a proactive role:
  - 56% want **regular cyber safety sessions.**
  - 22% recommend banning phones in schools.
  - 14% emphasize **joint sessions for parents and teachers.**
  - 8% want cyber safety integrated into the curriculum.

**3. School Authorities' Perspective**

- **89% government schools** participated in the research study.
- Teachers form the majority of respondents (72%), indicating ground-level insights, though principals (28%) are underrepresented.
- All schools (100%) have internet facilities and staff internet access—an opportunity as well as a risk.

**Policies and Practices**

- **83% schools have cyber safety policies,** but only 61% report implementation.
- **Cyber safety sessions** are conducted in 67% of schools, while 17% have never organized one.Parent workshops are limited as only 33% have conducted them, despite parents being key actors.
- **Reporting mechanisms** are heavily dependent on teachers (67%); only 5% offer confidential digital reporting.

**Challenges to address online crime against adolescents**

- Key barriers include:
  - Lack of awareness among staff (33%).
  - Rapid technological changes (22%).
  - Weak or unclear policy frameworks (20%).
  - Resource constraints (14%).

**Threats and cases of online crime against adolescents**

- Schools identify privacy breaches (20%), cyberbullying (19%), and screen addiction (19%) as major threats, followed by stranger danger (18%) and scams (16%).
- While **67% reported no cyber safety cases**, this could be due to **underreporting and weak reporting mechanisms** rather than absence of issues.

**Best Practices**

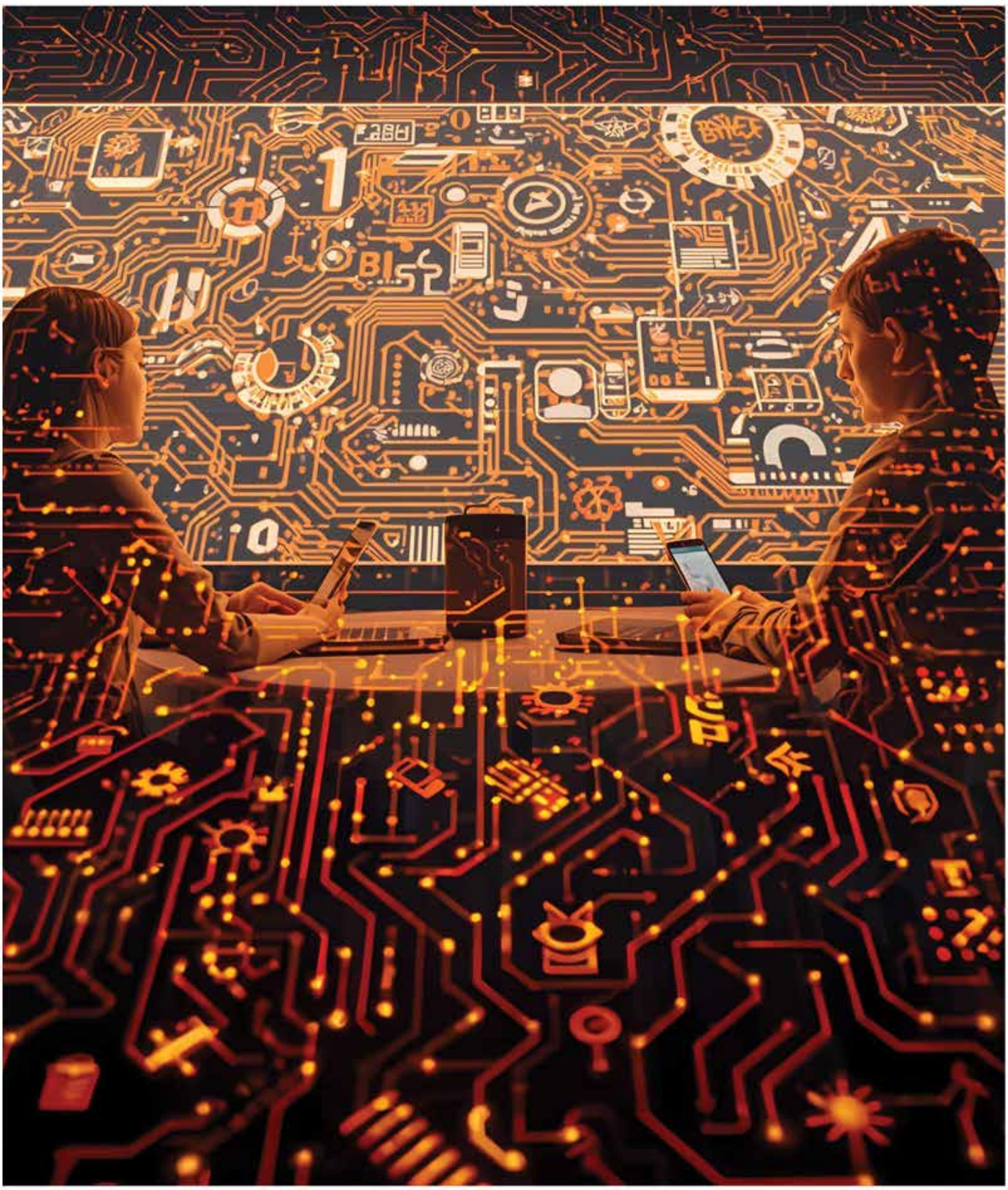
- 44% of schools shared best practices, mostly in the form of **awareness campaigns, role plays, or sensitization sessions.**

**4. Cross-Cutting insights**

1. **Awareness is not equal to safe practices –** Most adolescents know about cyber safety, yet risky behaviors (sharing personal info, poor password hygiene) remain widespread.
2. **Family is the first line of defense –** Parents are the most trusted source for adolescents facing cyber issues, but inconsistent monitoring and low digital literacy limit their effectiveness.
3. **Schools are key gatekeepers –** Policies exist in most schools, but implementation and child-friendly reporting systems are weak. Parents expect schools to do more.
4. **Psychosocial impact is rising –** sleep disorders, food behavior changes, and screen addiction reflect how cyber safety risks extend beyond the digital realm into health and well-being.
5. **Underreporting is a major challenge –** Many schools and parents claim “no cases” of cyber risks, but evidence from adolescents suggests otherwise, indicating fear, stigma, or lack of safe reporting channels.
6. **Multi-stakeholder collaboration is essential –** Schools, parents, NGOs, government agencies, and peers all play complementary roles. No single actor can ensure safety alone.
7. **Need for structured interventions –** Continuous awareness sessions, digital literacy programs, parental workshops, student peer leaders **(“Cyber Yodhas”)**, and external collaborations with experts are critical for sustainable impact.

# Descriptive Analysis

# Mapping the Digital Landscape of Adolescents



# Chapter 8: Mapping the Digital Landscape of Adolescents

**Gender-wise respondents**

The chart shows an equal gender distribution among participants, with 50% female (n=2400) and 50% male (n=2400). This balance indicates that the sample is gender-representative, ensuring that both male and female perspectives are equally captured in the study. Such parity is beneficial for comparative analysis, as it minimizes gender bias and allows for more reliable insights into gender-based differences.

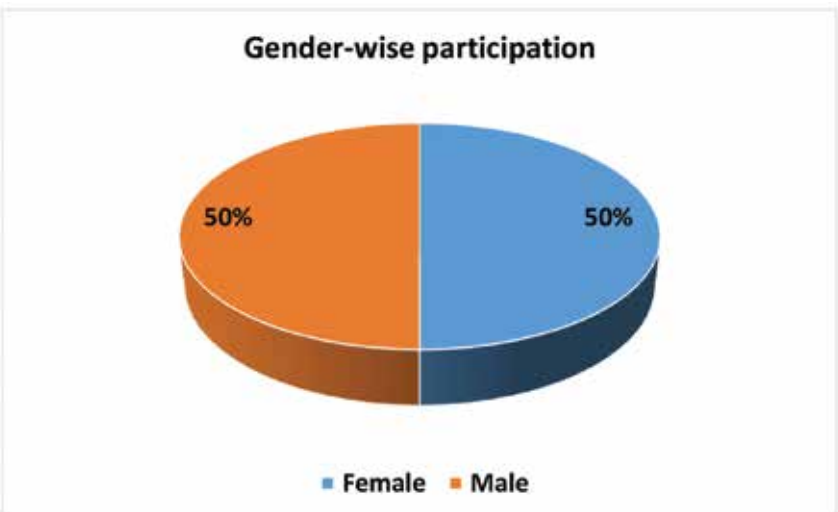



*Figure 12: Gender-wise participation*

**Educational status of respondents**

The majority of students belong to 9th–12th grade (40.95%), followed closely by those in 5th–8th grade (39.92%).A smaller proportion of participants are from below 5th grade (16.69%), while only 2.44% are pursuing studies above 12th (Graduation/BA/others).This distribution suggests that the dataset is **heavily weighted toward adolescents in middle and secondary school**, making it highly suitable for analyzing adolescent perspectives.

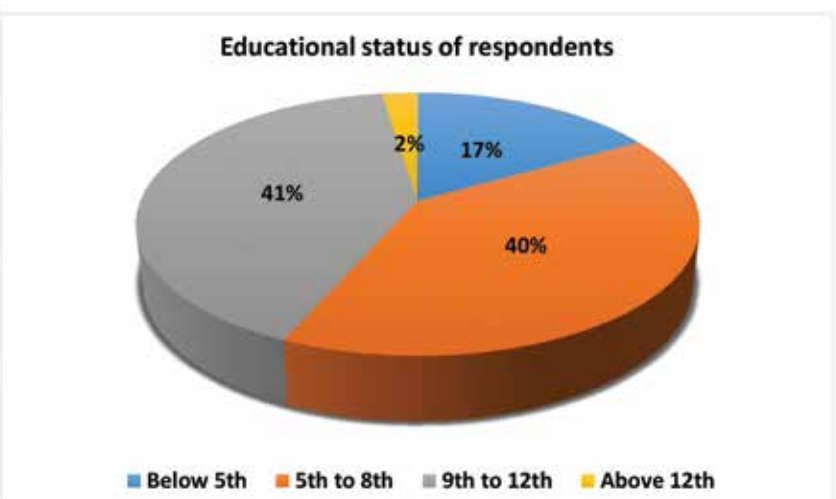



*Figure 13: Educational status of respondents*

**District-wise data respondents**

The chart presents the distribution of respondents across six regions: **South East, North West, West, Central, North East, and South**. Each region has been allocated exactly 800 respondents.

**Key Points:**

**1. Uniform sampling across districts**

The data shows a balanced sampling approach, with equal representation from each of the six regions.This ensures that no single region is over- or under-represented in terms of sample size.

**2. Total sample size**

With 800 respondents per district and 6 districts in total, the overall sample size is 4800 respondents.

**3. Implications for analysis**

This equal distribution allows for across regions without bias from unequal sample sizes.Findings can comparative analysisbe more reliably attributed to regional differences rather than differences in sample numbers.It strengthens the representativeness and credibility of regional comparisons in the study.

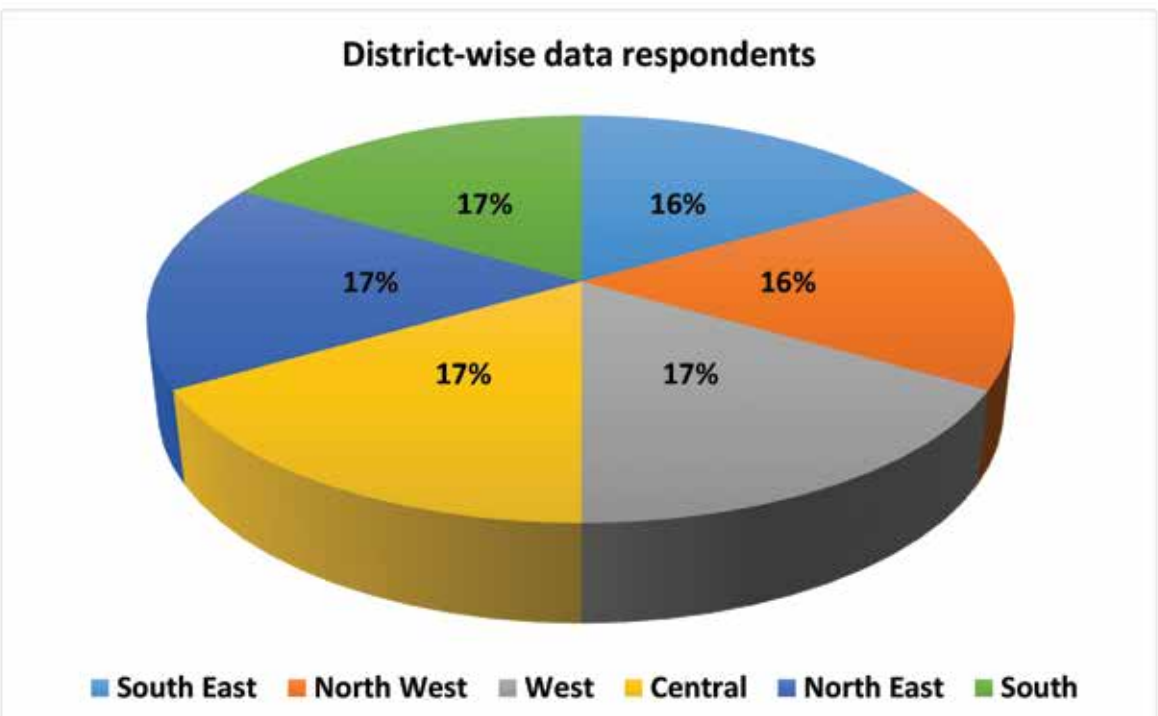



*Figure 14: District-wise data respondents*

**Accessibility of Internet at home**

Based on the data, a significant majority of the respondents have access to the internet at home. The frequency table shows that out of the total surveyed population, 84% individuals, reported having home internet access. In contrast, only 16% individuals, do not have internet access at home. This clear imbalance indicates that home internet connectivity is very common and widely available among this group.

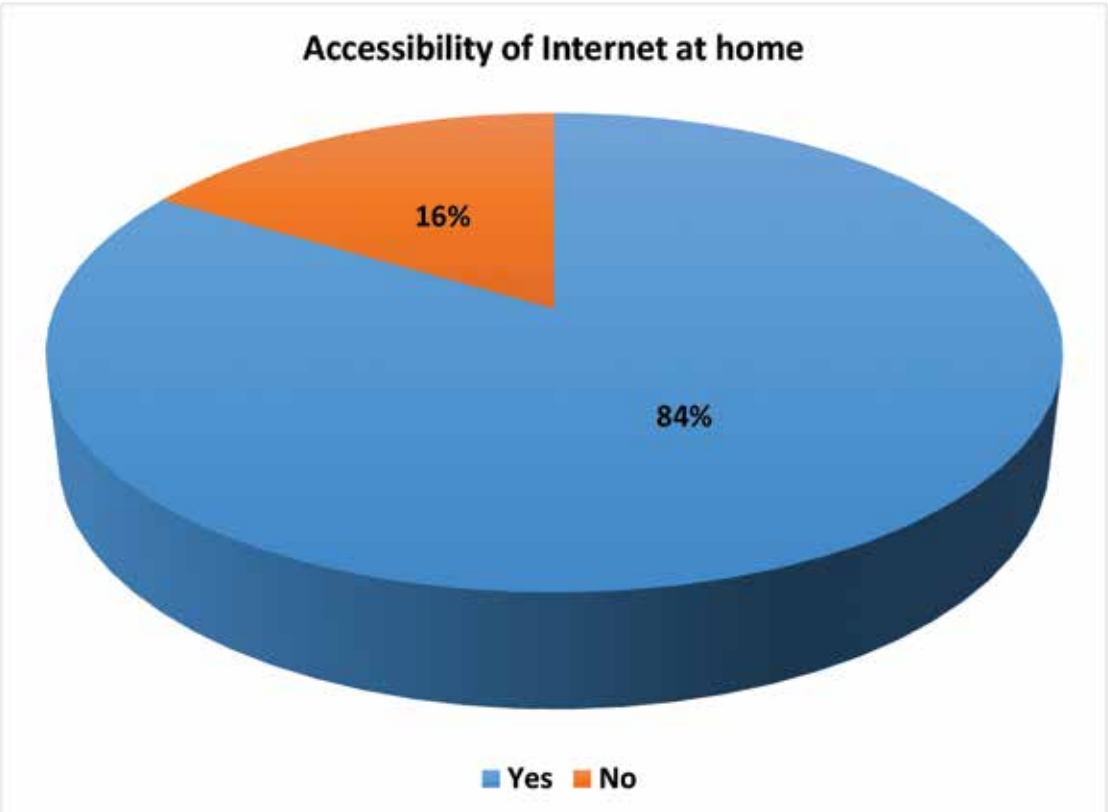



*Figure 15: Accessibility of internet at home*

**Device to access Internet**

Based on the data, a majority of the respondents, specifically 65%, have their own device to access internet. In contrast, the remaining 35% do not have their device. This shows that while a significant portion of the population is equipped with the necessary device, a substantial minority is not.

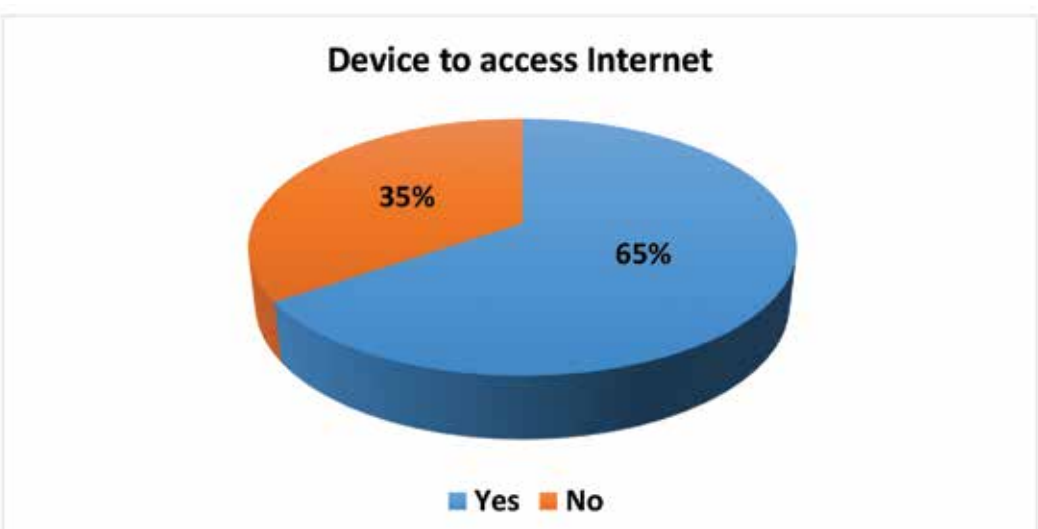



*Figure 16: Device to access internet*

**Whose Device is being used for Internet?**

The analysis of the data shows that mothers' devices are the most commonly used, accounting for 35% of the responses, followed by fathers' devices at 19.6%. Brothers' devices are used by 16.76% of the respondents, while sisters' devices account for 8.18%. In addition, 7.16% of the respondents reported using devices collectively referred to as grandparents." A smaller proportion rely on cousins' devices (2.56%) and other sources (5.60%). Overall, it is evident that parental devices (mother, father, and parents combined) make up the majority share of 89.26%, highlighting that children and adolescents largely depend on their immediate family members' devices, particularly their mothers, to access the internet.

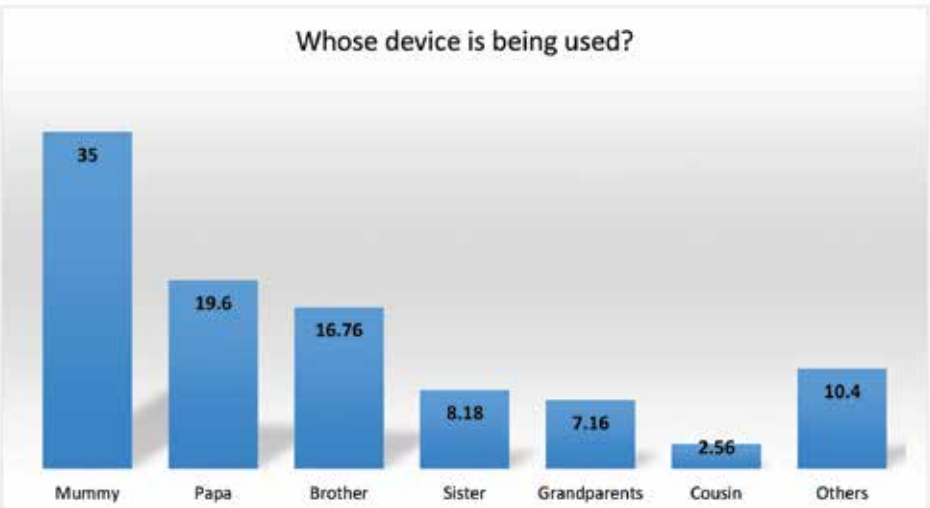



*Figure 17: Use of devices*

**Device usage categories for internet access**

The analysis clearly shows that smartphones dominate internet access, with 97.3% of respondents using them either alone or in combination with other devices. In contrast, laptops/computers are used by only 2.04%, while tablets (0.52%) and smart TVs (0.14%) have very limited use.

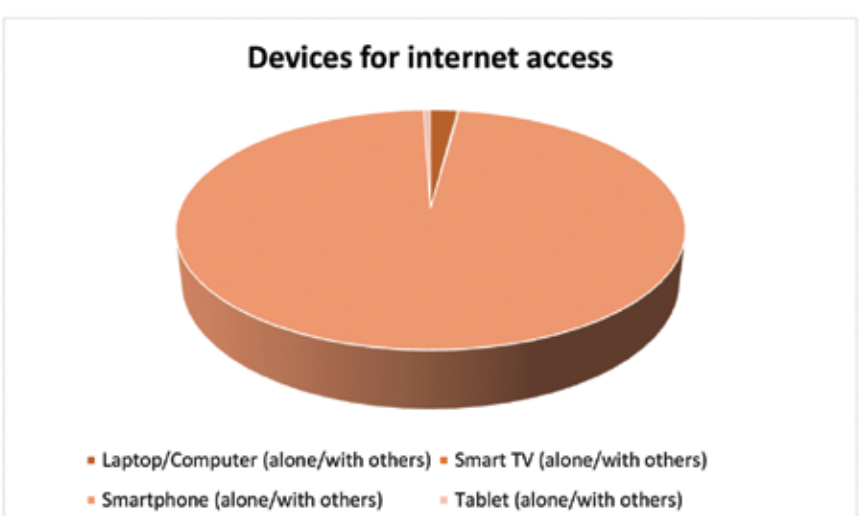



*Figure 18: Devices for internet access*

This highlights that smartphones are the primary gateway to the internet, reflecting accessibility, affordability, and convenience compared to other digital devices.

**Daily internet usage pattern**

The data reveals that the majority of respondents, 40.9%, spend 1 to 2 hours online daily (excluding schoolwork). This is followed by 25.13% who spend 3 to 4 hours online, while 20.12% reported using the internet for less than 1 hour per day. A smaller but notable share, 13.85%, spend more than 4 hours online daily. Overall, the findings indicate that while most adolescents maintain moderate daily internet use, a significant proportion are engaging for longer durations, which highlights both opportunities for learning and potential risks of excessive screen time.

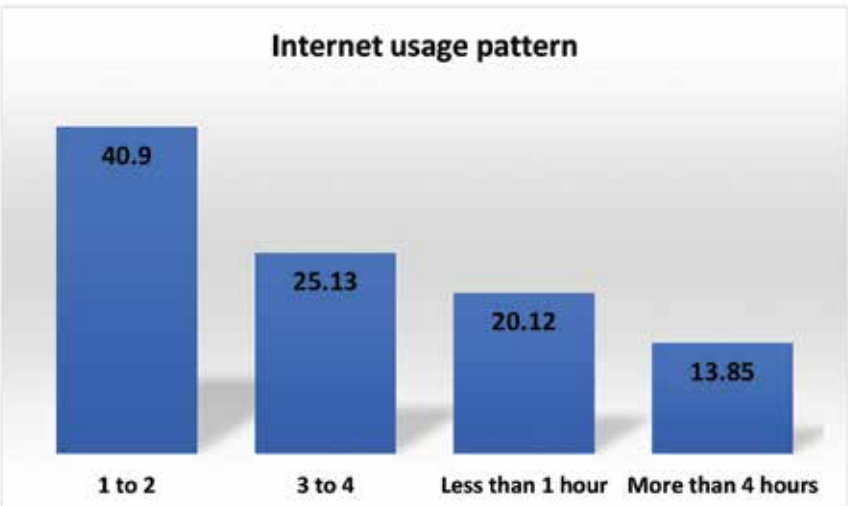



*Figure 19: Internet usage pattern*

**Prevalence of social media account ownership among adolescents**

The analysis shows that a majority of respondents, 61%, reported having their own social media account, while 39% do not. This indicates that more than half of the adolescents are actively engaged on social media platforms, highlighting the widespread penetration and influence of social media in their daily lives.

At the same time, a considerable proportion of respondents remain outside direct social media usage, which may be due to factors such as age restrictions, parental control, or personal choice. This distribution underlines the need to design awareness and safety interventions considering both active users and non-users, as the latter may still be indirectly exposed through shared or borrowed accounts.

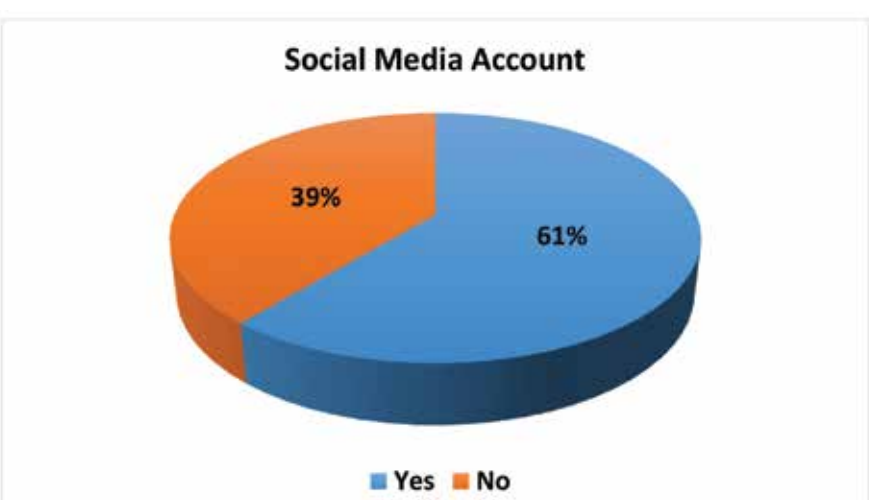



*Figure 20: Social Media Account*

The analysis shows that among adolescents without personal social media accounts as discussed above (39%), the majority rely on their mother's account (39%) and father's account (33%), together making up over 72% of cases. Smaller proportions use accounts of their sisters (10%) or brothers (9%), while 5% indicated using "personal" accounts in an informal/shared way, and 4% reported using accounts listed as "other family members."

This clearly highlights that parental accounts are the most common alternative for adolescents without their own accounts, followed by siblings' accounts, indicating both strong family dependence and limited digital autonomy.

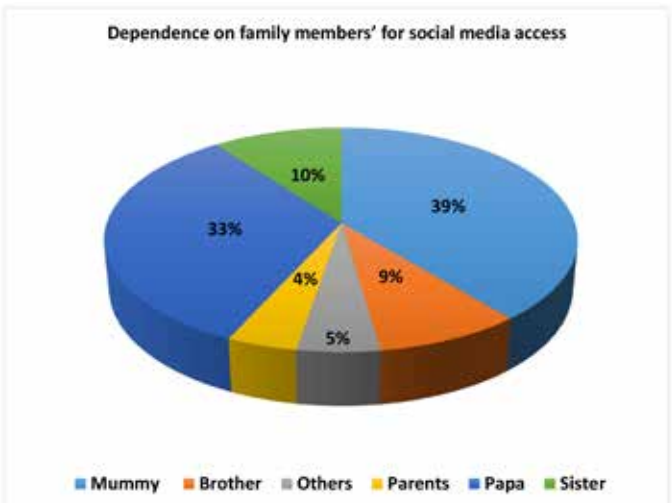



*Figure 21: Dependence on family members for social media access*

**Prevalence of multiple social media accounts among adolescents**

The data indicates that a majority of respondents, 65%, reported that they do not use more than one social media account on a single platform. In contrast, 35% of respondents admitted to maintaining multiple accounts on the same platform. This suggests that while most adolescents prefer to manage a single account for their online presence, a significant proportion—over one-third—engage in creating and using multiple accounts.

Such behavior may reflect varied purposes such as maintaining separate personal and public identities, experimenting with anonymity, or exploring social spaces with different peer groups. This finding highlights the need to better understand the motivations and potential risks associated with managing multiple accounts, especially in the context of cyber safety and responsible online behavior.

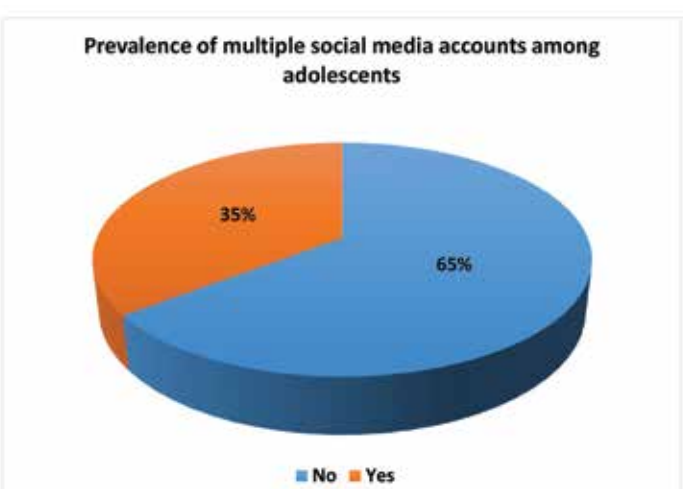



*Figure 22: Multiple social media accounts*

**Why adolescents use multiple social media accounts?**

44.36%adolescents use social media for fun, reels, chatting, videos, and connecting with friends.15.79%reported reasons like forgetting passwords, account bans, or managing only one account due to access difficulties. 6.02% adolescents manage multiple accounts for privacy, safety, or separating personal and public use. 6.01% explicitly mentioned using multiple accounts to increase followers, gain popularity, or manage different public/private identities. 2.26% mentioned using accounts for learning, gaining knowledge, or skill development. A considerable percentage of responses (25.56%) were vague, unclear, or not directly classifiable.

This distribution clearly shows that entertainment dominates adolescent social media use, while privacy, popularity, and learning form smaller but important dimensions.

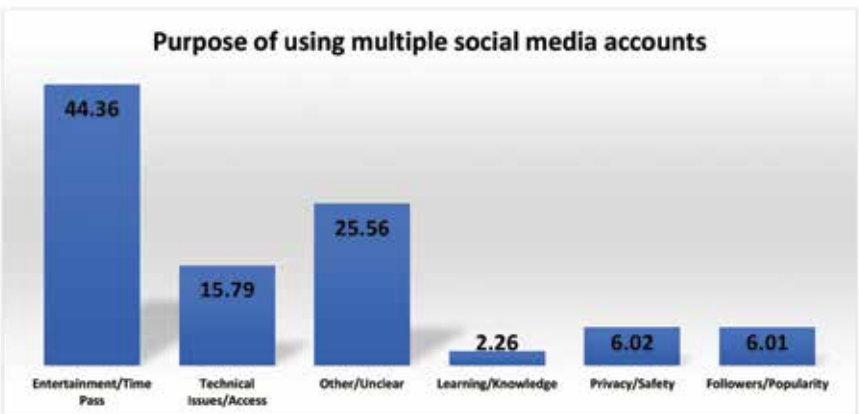



*Figure 23: Purpose of social media accounts*

**Adolescents preferred digital platform**

The analysis shows that YouTube/Streaming dominates adolescents' digital activities with 28.2%, reflecting their strong inclination toward video-based entertainment and content consumption. Messaging apps such as WhatsApp, Telegram (20.51%) and social media platforms like Instagram, Facebook, and Snapchat (17.95%) also play a central role, highlighting the importance of communication and peer connectivity in their daily digital lives.

A smaller proportion is engaged in online games (10.26%), which points to recreational use, while educational platforms (5.13%) remain comparatively underused, showing that learning is not yet a primary digital driver. Other responses (17.95%) indicate varied or unclear digital behaviors outside the main categories.

Overall, the data reveals that adolescents' online engagement is predominantly entertainment and communication-driven, with only a limited focus on education-oriented platforms.

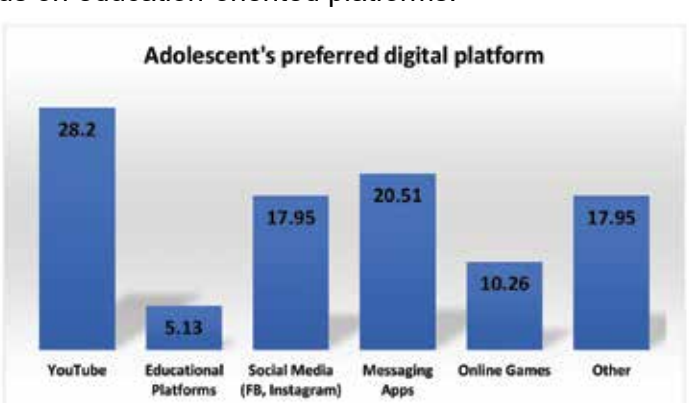



*Figure 24: Preferred digital platform*

**Appropriate-age for using social media**

The data indicates that the largest proportion of respondents, 39%, believe the appropriate age for using social media is 15–17 years. This is followed by 32% who feel it should be 17 years and above, reflecting a significant group that prefers stricter age thresholds for social media use. Meanwhile, 24% suggest that adolescents aged 13–15 years can begin using social media, aligning with global practices where 13 is often the minimum legal age for account creation. Only 5% of respondents think that children as young as 10–13 years should be allowed access.

“Overall, the findings highlight that a majority of respondents (over 70%) support restricting social media use to 15 years or older, signaling a strong awareness of potential risks and the importance of maturity before engaging in online platforms. This perspective underlines a cautious approach toward early exposure, balancing digital access with safety and responsible usage”.

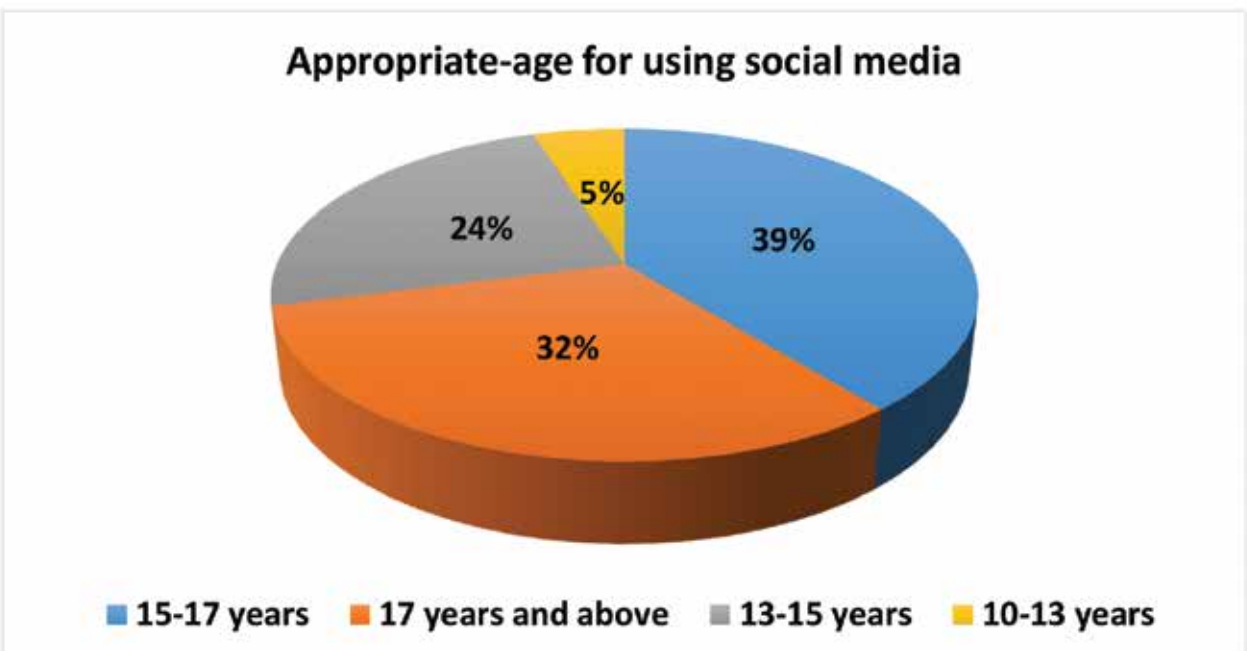



*Figure 25: Appropriate-age for social media*

**Appropriate-age for using mobile phones**

The data shows that the majority of respondents, 36%, consider 15–17 years as the most appropriate age for using a mobile phone, followed by 26% who believe it should be 17 years and above. Together, this indicates that over 62% of respondents favor restricting mobile usage until mid-to-late adolescence, highlighting concerns around early exposure and responsible use.

At the same time, 20% feel that children aged 13–15 years are ready to use mobile phones, while 13% support access for those between 10–13 years. A smaller share, 3%, suggest that children can start as early as 8–10 years, and very few respondents (1% for 5–8 years and 1% for below 5 years) approve of mobile use in early childhood.

Overall, the findings suggest that the community strongly associates mobile phone usage with later adolescence, with most respondents prioritizing maturity, responsibility, and digital readiness over very early exposure. This reflects awareness of both the opportunities and risks linked with mobile phoneuse among children and adolescents.

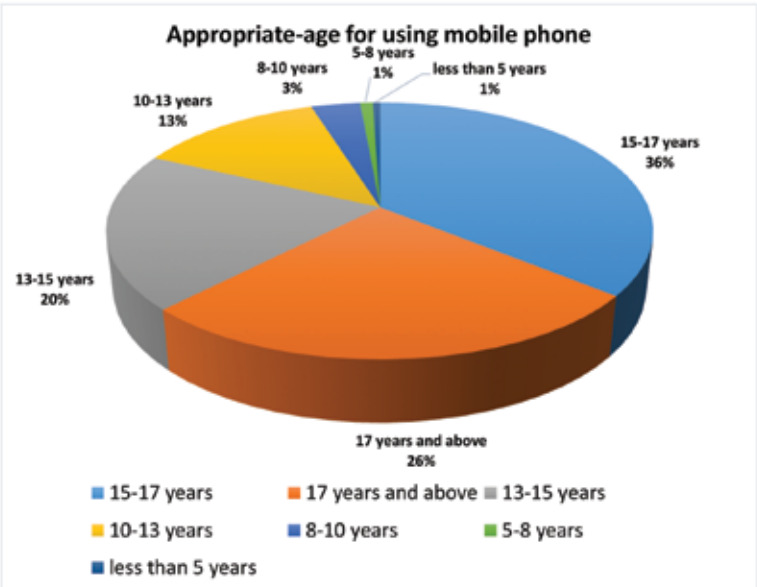



*Figure 26: Appropriate age for mobile phones*

**Awareness of the term "Cyber Safety" among respondents**

The data indicates that a significant majority of respondents, 84%, have heard of the term "cyber safety" or "internet safety", showing a high level of awareness among the participants. This suggests that most adolescents and community members are at least familiar with the concept, which is an encouraging sign for promoting safe digital practices.

On the other hand, 16% of respondents reported that they have never heard of the term, highlighting a critical knowledge gap. This group represents a vulnerable section that may lack the necessary understanding to protect themselves from online threats, misinformation, or unsafe practices.

Overall, while the majority are aware of cyber safety, the presence of a sizeable minority with no awareness underlines the need for targeted awareness campaigns and educational interventions to ensure that every individual, especially adolescents, understands the basics of internet safety. This would help in building a more secure and informed digital community.

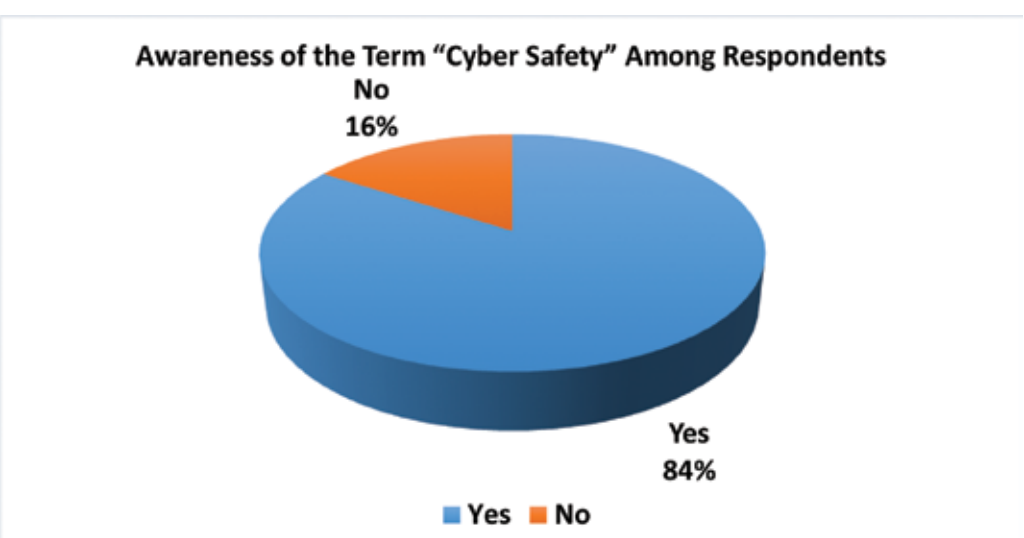



*Figure 27: Awareness about Cyber Safety*

**Source of Information about Cyber Safety**

The analysis of the data reveals that the school curriculum is the strongest source of cyber safety awareness, contributing 28% of the responses, which highlights the critical role of formal education in shaping knowledge and practices around safe internet use. Parents and guardians (14%) and news/media (13%) also play an important role, showing that both family influence and mass communication significantly contribute to awareness. Friends (12%) and social media platforms (9%) further emphasize the impact of peer networks and the digital environment itself in shaping perceptions of online safety. Meanwhile, NGOs (12%) and online educational platforms (6%) provide supplementary knowledge, often addressing gaps left by mainstream sources. The "Other" category (6%)indicates that diverse informal avenues also contribute meaningfully. Overall, the findings suggest that cyber safety awareness is a multi-dimensional process, shaped not only by schools but also by families, peers, media, and civil society actors, underscoring the need for a collaborative, multi-stakeholder approach to building a safer digital environment.

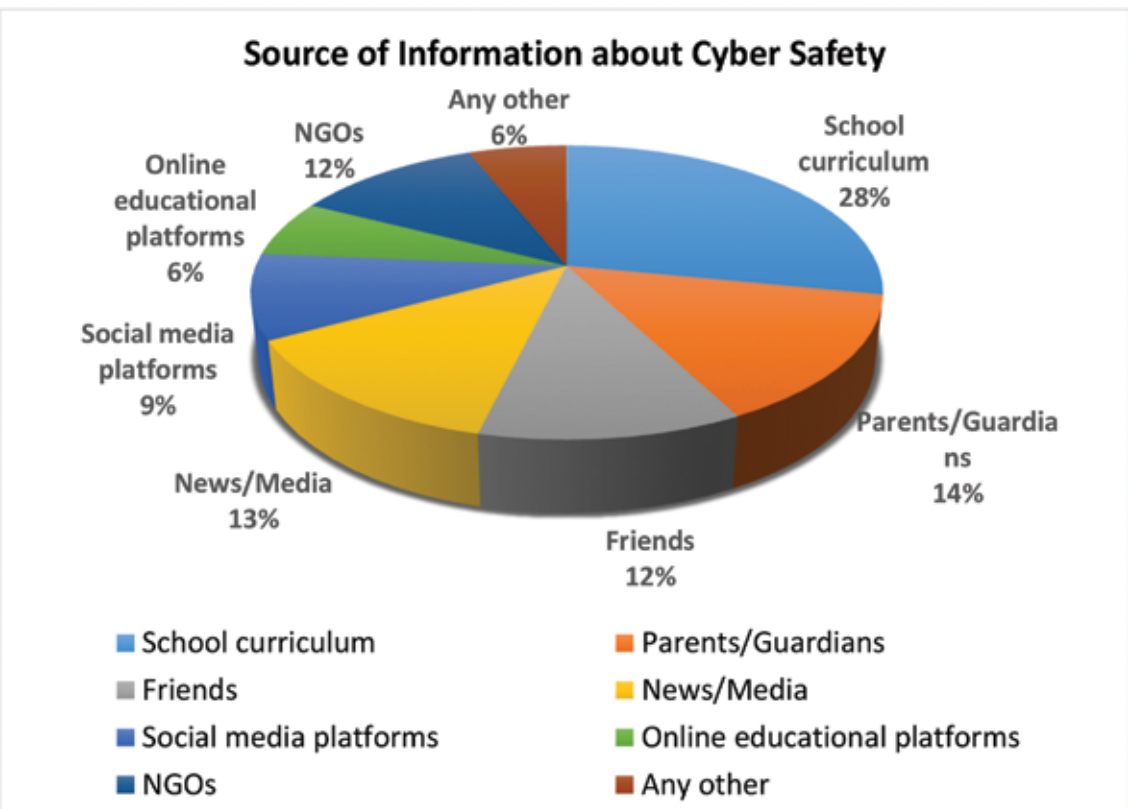



*Figure 28: Source of information about cyber safety*

**Recognized measures for safe online behavior**

The analysis reveals that the most widely recognized cyber safety practice is not sharing passwords/OTP (28.7%), highlighting strong awareness among adolescents regarding password security. This is followed by avoiding strangers online (18.3%) and identifying fake news (12.9%), reflecting growing awareness of digital risks. A significant portion of respondents also chose multiple combined responses (18.8%), indicating that many adolescents view cyber safety as a multi-dimensional concept rather than a single practice. Comparatively, practices like using antivirus software (7%), managing screen time (7.4%), and reporting cyberbullying (4.9%) were less prioritized, suggesting areas where further awareness is needed. Only a small fraction (2%) admitted to having no knowledge of cyber safety.

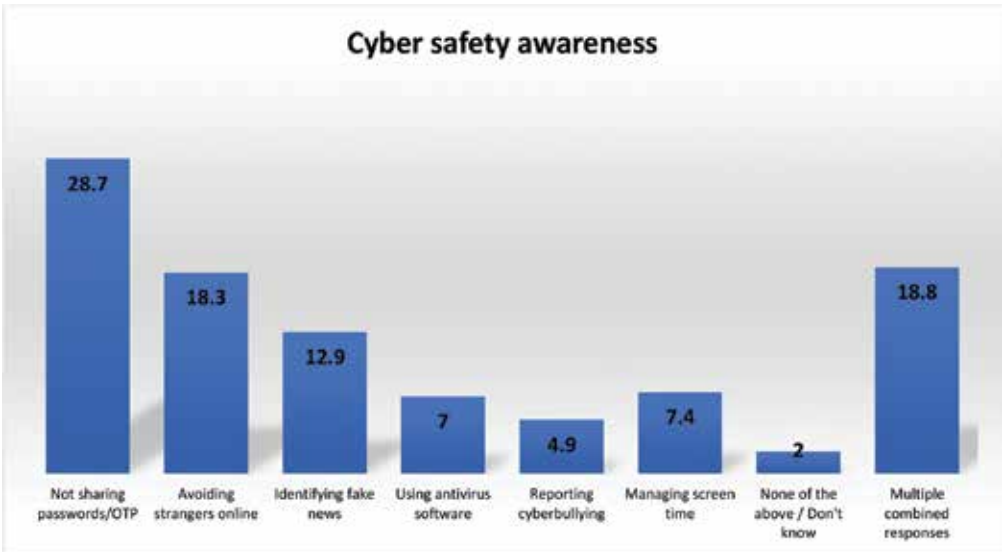



*Figure 29: Cyber safety awareness*

**Adolescents' practice of sharing personal information online**

The data reveals that a majority of adolescents (59%) have never shared personal information online, indicating a relatively good level of awareness regarding privacy and cyber safety. However, a significant proportion, 32%, admitted to having shared sensitive details such as address, school name, phone number, or photographs. This reflects a concerning vulnerability to online risks such as identity theft, cyberbullying, or exploitation. Additionally, 9%of respondents were not sure whether they had shared such information, suggesting a lack of clarity or awareness about what constitutes "personal information".

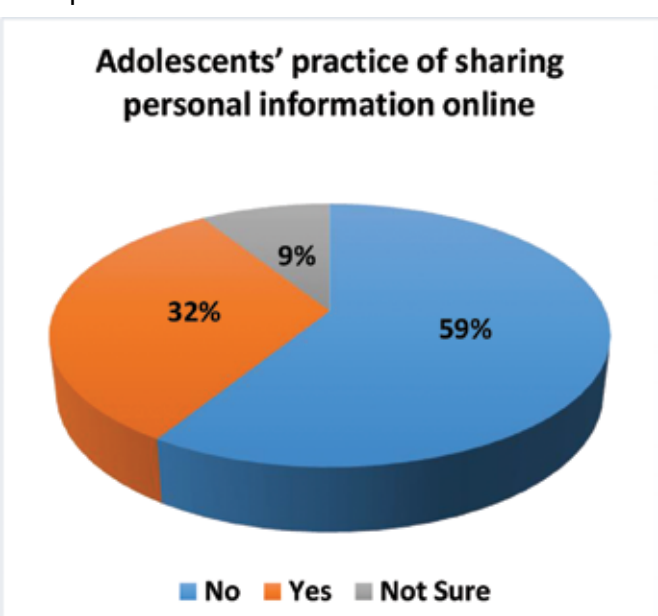



*Figure 30: Sharing of personal information online*

**Adolescents' practice of accepting friend requests from strangers**

The findings reveal that 59% of adolescents reported they never accept friend/follow requests from strangers on social media, showing a cautious approach to online interactions. Meanwhile, 35% of respondents indicated that they sometimes accept such requests, reflecting a moderate level of risk exposure. A smaller proportion, 6%, stated that they always accept friend requests from strangers, highlighting a critical area of vulnerability.

Overall, while the majority demonstrate safe online practices, the 41% who sometimes or always accept requests represent a significant group needing targeted cyber safety awareness and behavior change interventions.

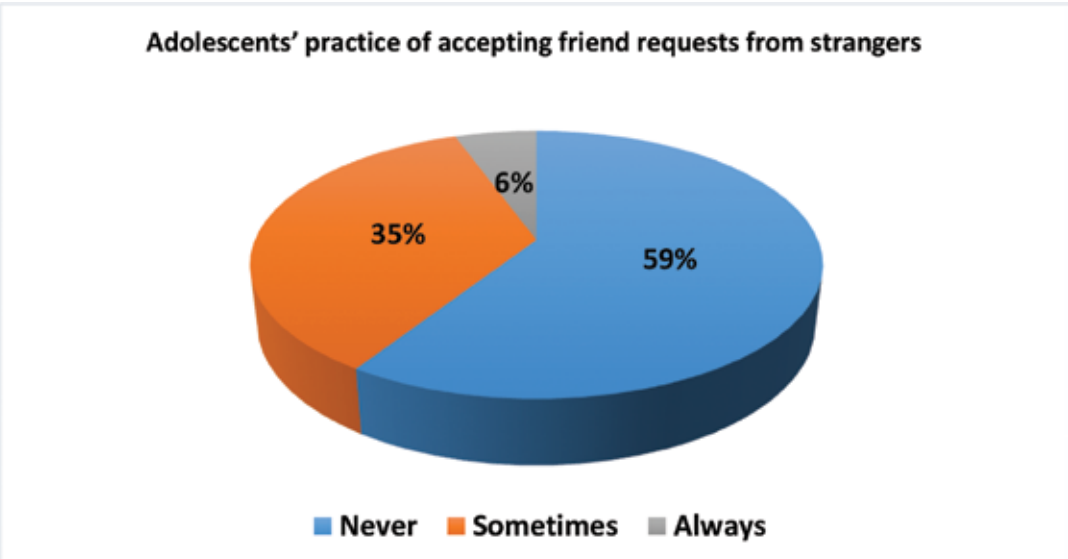



*Figure 31: Accepting friend requests from strangers*

**Adolescents' use of privacy settings on social media**

The findings reveal that 46% of adolescents actively use privacy settings on their social media accounts, reflecting a fair level of awareness regarding online safety measures. On the other hand, 40% do not use privacy settings, exposing themselves to potential risks such as misuse of personal data, online harassment, and cyber threats. Furthermore, 14% of respondents reported that they are unaware of privacy settings, which highlights a clear knowledge gap among young users.

These insights emphasize the importance of strengthening digital literacy and practical awareness campaigns so that more adolescents can safeguard their online presence effectively.

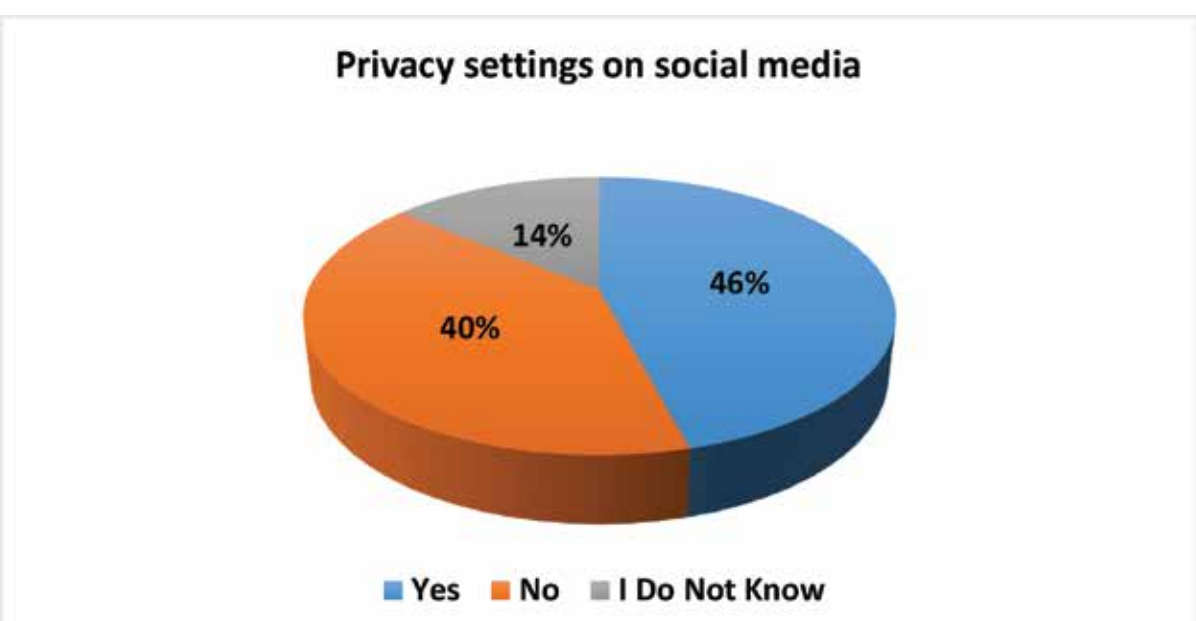



*Figure 32: Privacy settings*

**Adolescents' frequency of changing passwords**

The data indicates that a significant proportion, 46%, of adolescents never change their passwords, leaving their accounts highly vulnerable to hacking and unauthorized access. About 23% reported that they rarely update their passwords, which, while slightly better, still reflects poor password hygiene. Meanwhile, 17% of adolescents change their passwords every few months, and only 15% follow a relatively safe practice of updating passwords once a month.

These findings suggest that while a small group is adopting safer digital practices, the majority of adolescents are still neglecting this fundamental aspect of cyber safety, highlighting the urgent need for awareness and habit-building around password security.

This indicates that while a small group is practicing better password hygiene, the majority still demonstrate risky online behavior, which could make them more susceptible to hacking and unauthorized access. Strengthening awareness on the importance of regular password updates is therefore essential.

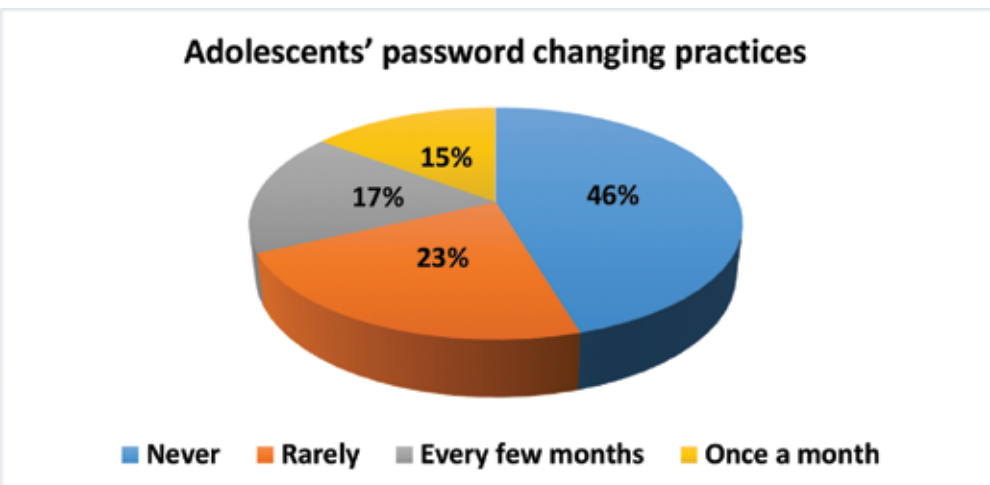



*Figure 33: Password changing practices*

**Adolescents' experience with suspicious online links**

The findings reveal that a large majority, 43%, of adolescents reported that they have never clicked on suspicious links or ads online, which reflects a generally cautious approach while browsing the internet. However, 38% were

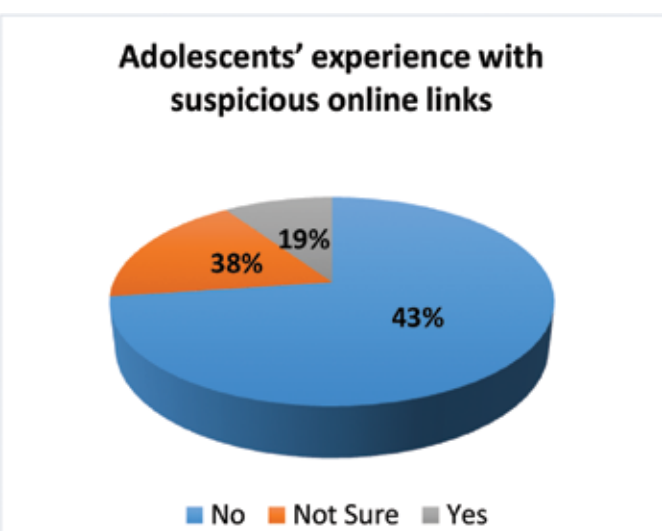



*Figure 34: Experience with suspicious online links*

not sure whether they had done so, indicating a lack of awareness about what constitutes a suspicious link and the potential risks associated with it. Worryingly, about 19% admitted to having clicked on such links, exposing themselves to possible cyber threats like malware, phishing, or identity theft.

This highlights that while many adolescents are alert to online risks, a significant portion either lack clarity or engage in risky behaviors, underlining the need for stronger digital literacy and awareness campaigns.

**Exposure to online risks among adolescents**

The analysis reveals that a majority of adolescents (54%) reported not facing any online risks, suggesting a significant proportion remain safe in their digital interactions. However, 12% experienced cyberbullying, while 10% reported being asked to share personal photos or videos, both highlighting concerning trends in online safety. Additionally, 9% faced online scams or frauds, hacking or account theft (7%) and receiving inappropriate content (8%). This indicates that a considerable segment of adolescents faces overlapping challenges in cyberspace.


*Figure 35: Online risks faced*

The percentage distribution underlines the urgent need for awareness and preventive interventions to address cyberbullying, online exploitation, and digital frauds while strengthening digital literacy and resilience among adolescents.

**Reporting of cyber-crime**

The findings highlight that more than half (56%) of respondents have never reported a cyber-crime, reflecting a significant gap in awareness or willingness to approach formal channels. On the other hand, 34% acknowledged reporting cybercrimes, which indicates that about one-third of participants are proactive in seeking redressal when faced with online threats. Meanwhile, 10% preferrednot to disclose their stance, suggesting either hesitation, lack of trust in reporting mechanisms, or discomfort in sharing their experiences.

This pattern suggests that while a section of respondents is aware and responsive, a large proportion either avoids or hesitates to report, underlining the need for awareness drives on safe, confidential, and supportive cybercrime reporting systems.

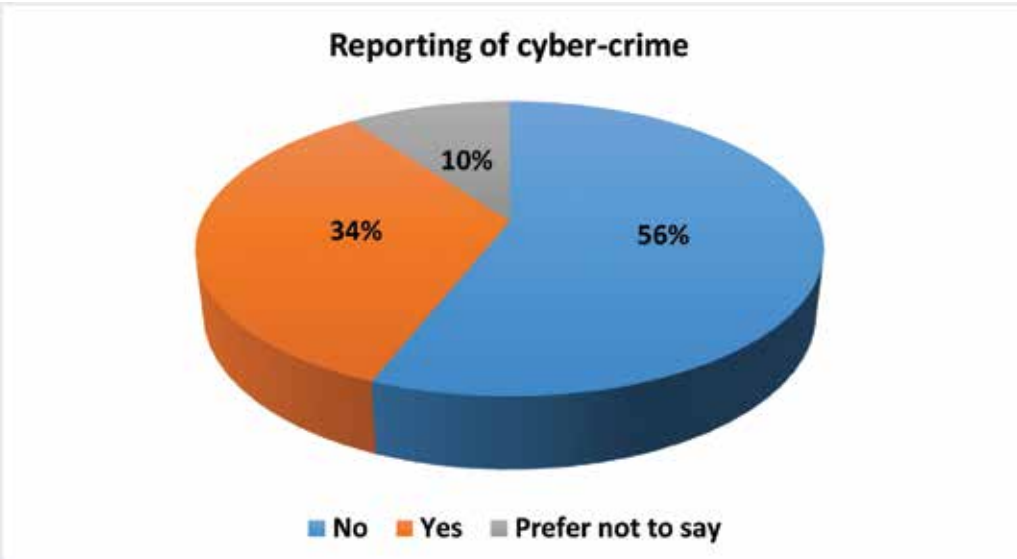



*Figure 36: Cybercrime reporting*

**Reporting ofcyber issues: Whom do respondents approach?**

The analysis shows that parents are the most trusted source of support, with over half of respondents (54.2%) reporting cyber issues to them. A smaller proportion turn to friends (11%) or teachers (8.7%), while relatives (7%) are even less likely to be approached. Interestingly, about 12.8% of respondents seek formal help from the police or cyber cells, whereas NGOs/social workers account for only 5.8%. A negligible 0.5% of respondents indicated they would not report to anyone.

This clearly highlights that families remain the first line of response in cyber-related concerns, while institutional or external mechanisms like police or NGOs are approached by a smaller fraction of individuals.

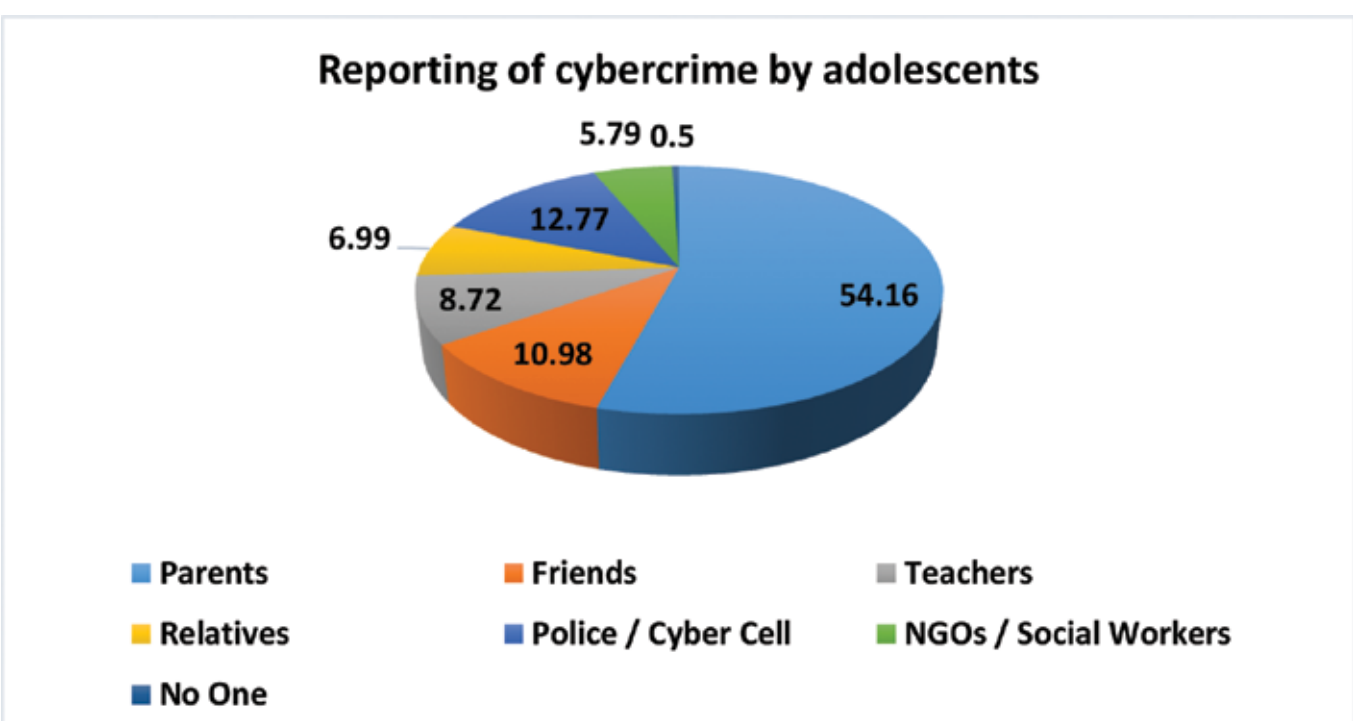



*Figure 37: Respondents for cybercrime reporting*

**How confident are users in navigating the Internet?**

The results show that the majority of respondents feel confident about navigating the internet. Around 36% said they are somewhat confident, and 32% reported being very confident. Together, this indicates that about 7 in 10 respondents feel confident online.In contrast, 20% were not sure about their abilities, while 12% admitted they are not confident.

This highlights that although confidence is generally high, there is still a considerable group — roughly one-third — that could benefit from digital literacy support and awareness programmes to strengthen their online navigation skills.

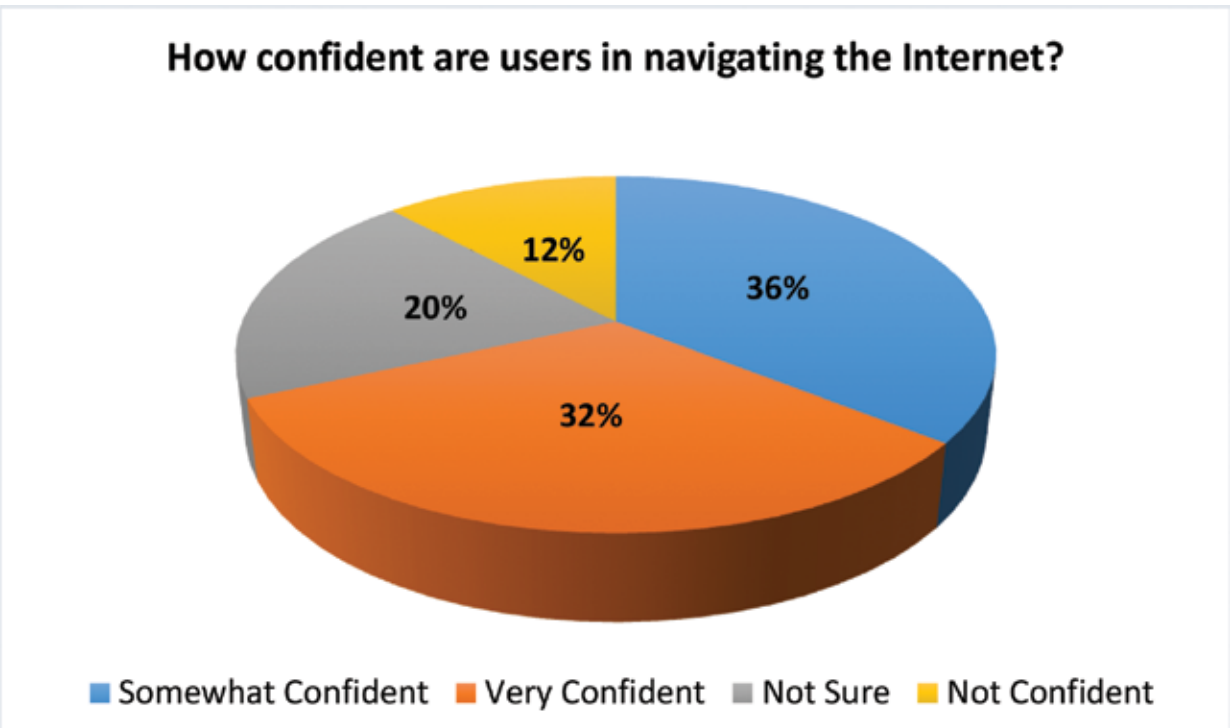



*Figure 38: Confidence in navigating the internet*

**Reasons for lack of confidence in using the Internet**

The chart shows that the majority of respondents (71%) did not cite any specific reason for their lack of confidence in using the internet. This suggests either hesitation in sharing concerns or limited awareness about the challenges they face.

Among the stated reasons, lack of knowledge or unawareness (7%) and fear of hacking or misuse of data (7%) are equally highlighted as the primary factors behind insecurity. A smaller proportion expressed concerns about exposure to inappropriate content or addiction (4%), while neutral or balanced views (3%) indicate that some respondents neither feel strongly confident nor insecure.

Interestingly, 8% of responses fall under miscellaneous or scattered reasons, showing diverse but less common issues.

The findings reveal that while a majority refrain from expressing specific reasons, those who do mainly point to digital illiteracy and fear of cyber risks as the key barriers to internet confidence.

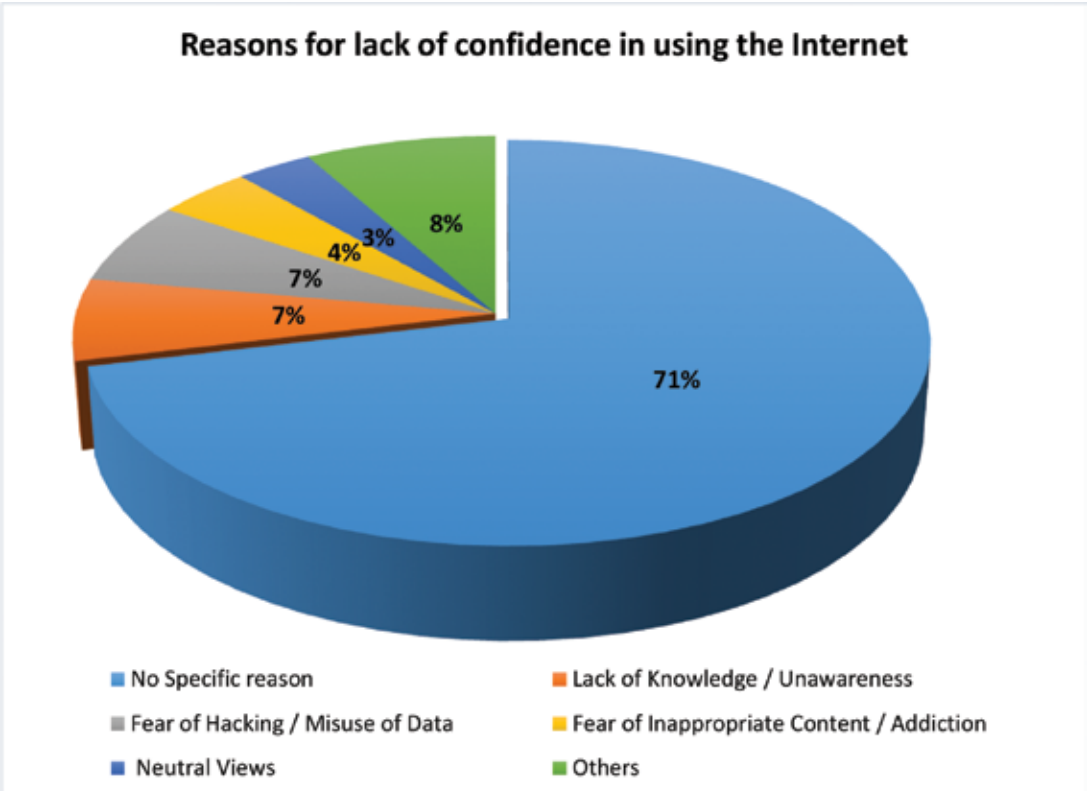



*Figure 39: Reasons for lack of confidence*

**School's role in cyber-safety awareness**

The majority of respondents, 70%, believe that their school provides sufficient guidance and awareness on online cyber safety. This indicates that schools are playing and can play a positive role in sensitizing students about safe internet practices.

However, around 30% of respondents feel that their schools do not offer enough guidance. This highlights a gap where additional efforts are needed to strengthen cyber safety education and ensure that all students are adequately informed.

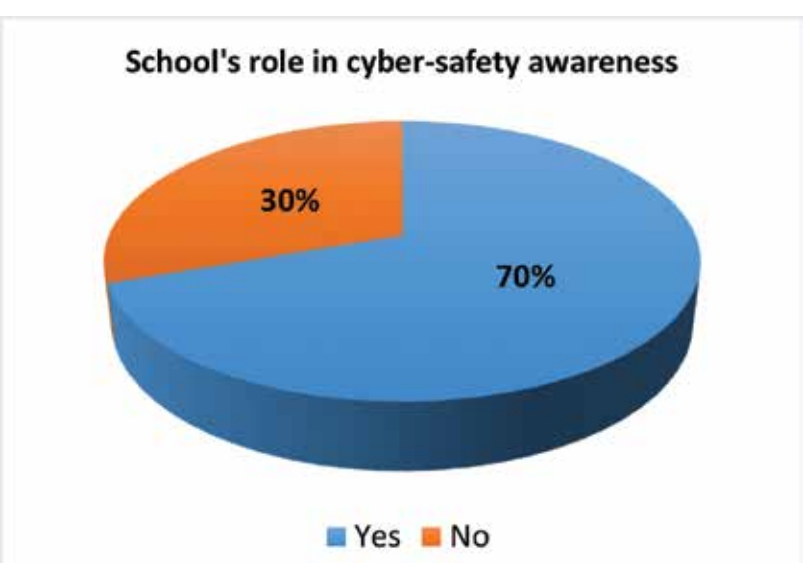



*Figure 40: School's role in cyber-safety*

The findings suggest that while schools are actively contributing, there remains a significant proportion of students who require more structured awareness programs.

**Perception of seriousness of cyber-safety issues**

A significant majority, about 70%, consider cyber safety issues to be very serious, reflecting a strong awareness of the potential risks and threats associated with unsafe online behavior. Additionally, 16% perceive the issue as somewhat serious, showing that while they recognize the importance, they may not view it as critically urgent. On the other hand, 8% of respondents are unsure about the seriousness of the matter, while around 6% believe it is not serious.

The findings highlight that most respondents understand the gravity of cyber safety concerns, but there remains a small segment that requires more

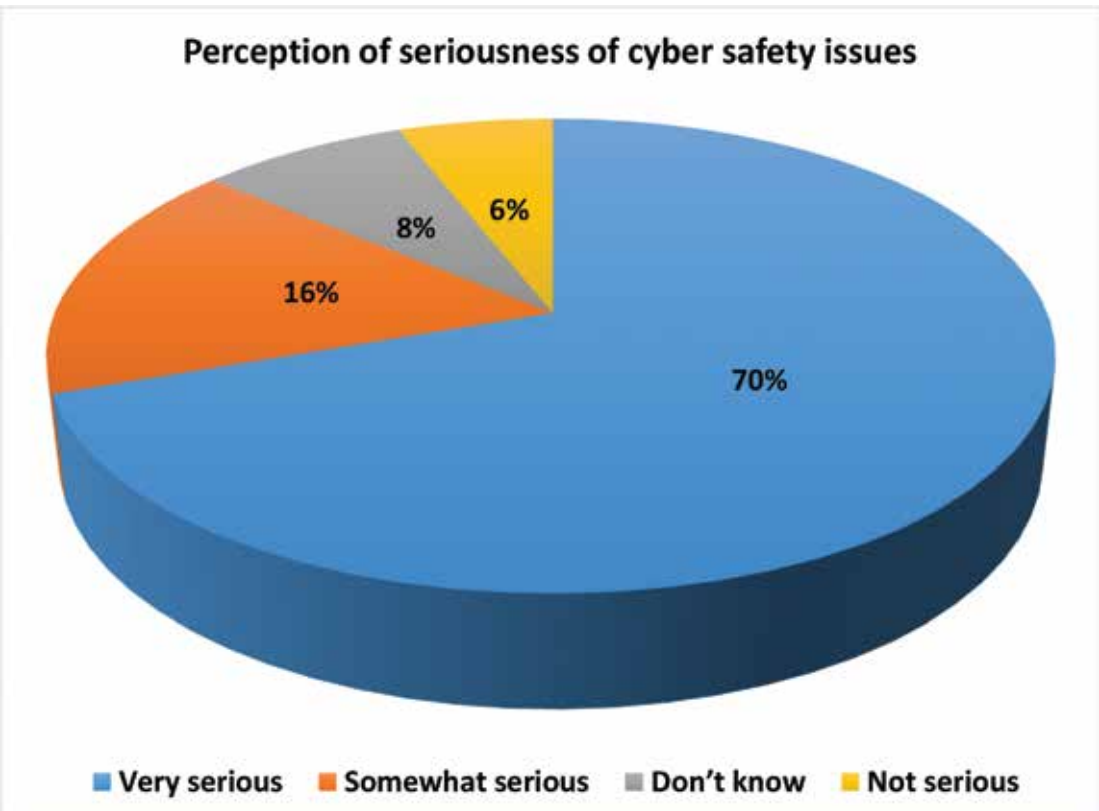



*Figure 41: Seriousness of cyber safety issues*

# Parental Perspective on Adolescents' Cyber Safety

# Chapter 9: Parental Perspective on Adolescents' Cyber Safety

**Age-group of respondents**

The age profile of the respondents reveals some important highlights. Half of the parents (50%) are below 30 years, showing that the majority of adolescents in this study are raised by very young parents. This is significant because younger parents are often more digitally connected and may have a better understanding of the online platforms their children use. At the same time, over three-fourths of the parents (77%) are younger than 40, which underscores that adolescent parenting in this sample is largely concentrated among a younger generation. In contrast, only 20% of parents are between 41 and 50 years, and a very small proportion, just 3%, are above 50 years. These figures suggest that while younger parents may be more aware of technology, older parents—though fewer—might face greater challenges in keeping pace with the digital risks their children encounter. This highlights the need for targeted cyber safety awareness programs, where younger parents can be guided to balance digital freedom with effective monitoring, and older parents can be supported to strengthen their digital literacy.

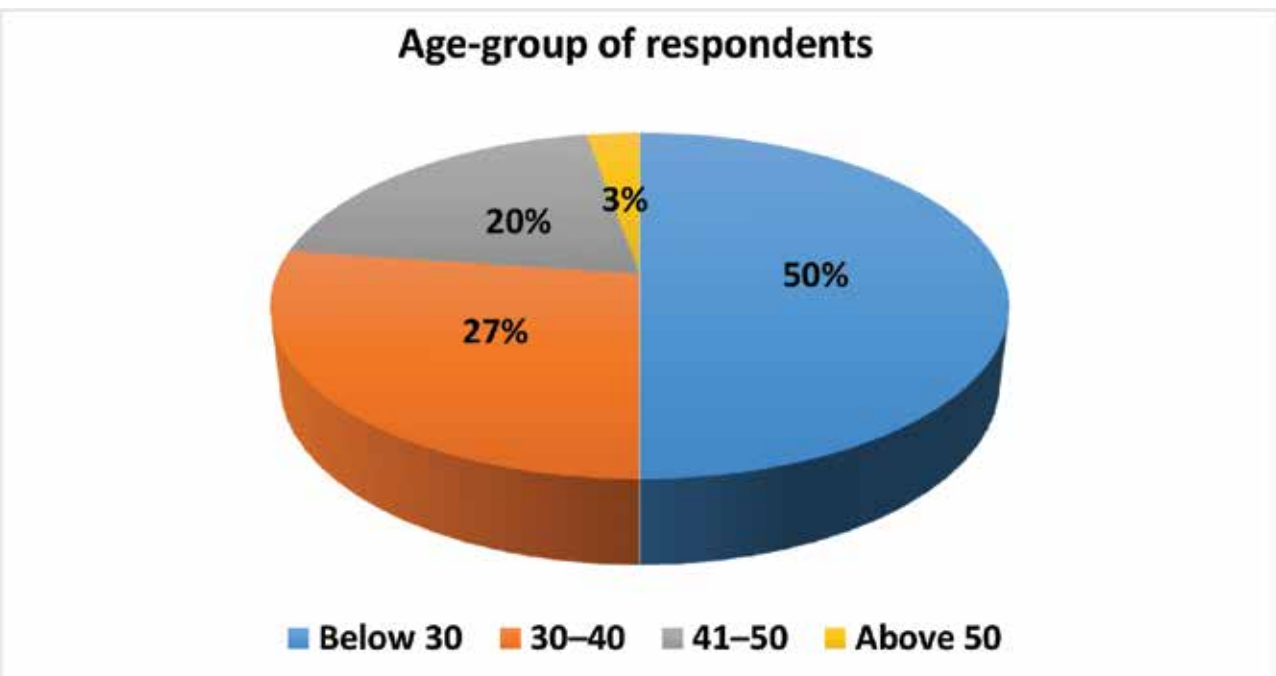



*Figure 42: Age-group of respondents*

**Gender-wise respondents**

Out of the total participants, females constitute more than two-thirds (69%), while males form less than one-third (31%). This indicates a 2.2:1 ratio of female to male participation. The data suggests that female caregivers were more responsive or more directly engaged in issues concerning adolescents' cyber safety.

In many household surveys, women tend to participate more actively due to their availability at home or greater willingness to engage in child-related issues. The 69% female participation here mirrors that trend. However, if we compare this with ideal household decision-making, where both parents should be equally involved, the under-participation of men highlights a gap that might influence how rules, monitoring, and communication about cyber safety are actually enforced at home.

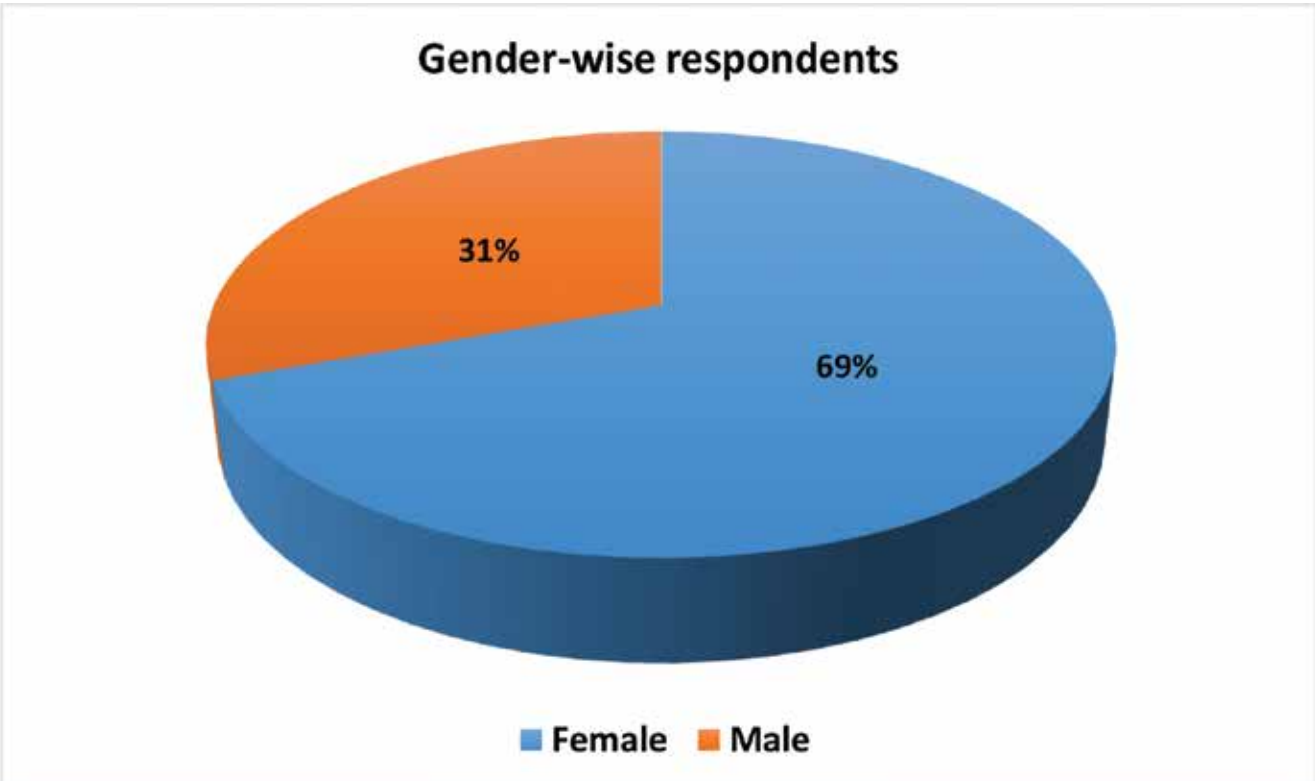



*Figure 43: Respondent's gender*

**Occupation of Respondents**

- **Homemakers dominate (61%):** The majority of respondents are women engaged in household work, reflecting the traditional gendered roles in the sample.
- **Private/Informal Jobs (20%):** A significant portion are engaged in small jobs or private-sector informal employment, showing economic dependence on non-regularized work.
- **Skilled/Professional roles (8%):** Although smaller, this group highlights some presence of specialized occupations (teachers, accountants, electricians, etc.).
- **Self-Employed/Business (5%):** A small proportion run their own businesses, shops, or are self-employed, indicating entrepreneurial activity.
- **Labour/Daily Wage workers (3%):** Represent the economically vulnerable segment dependent on daily wage employment.

- **Unemployed/Domestic (2%):** Reflects a small but notable group without formal work.
- **Students (1%):** Very few respondents are currently studying, possibly due to the focus on parents in this dataset.

This distribution shows that the majority are homemakers, with only about one-third engaged in income-generating activities, mostly in informal sectors. It highlights both gendered divisions and the reliance on non-regularized jobs within the community.

**Educational Status of Respondents**

- The largest group (32%) of respondents studied between 5th–10th standard, showing a moderate basic education level.
- 22% are below 5th standard, reflecting limited literacy and early school dropouts.
- 17% reached 10th–12th, suggesting that a fair share of parents attained secondary/higher secondary education.
- Around 21% (Undergraduate + Postgraduate) achieved higher education, which is a significant minority and indicates potential for informed awareness on digital issues.
- 8% are illiterate, showing that a small segment lacks formal education.

Overall, while more than half (54%) of parents have education up to 10th standard or below, only one-fifth have

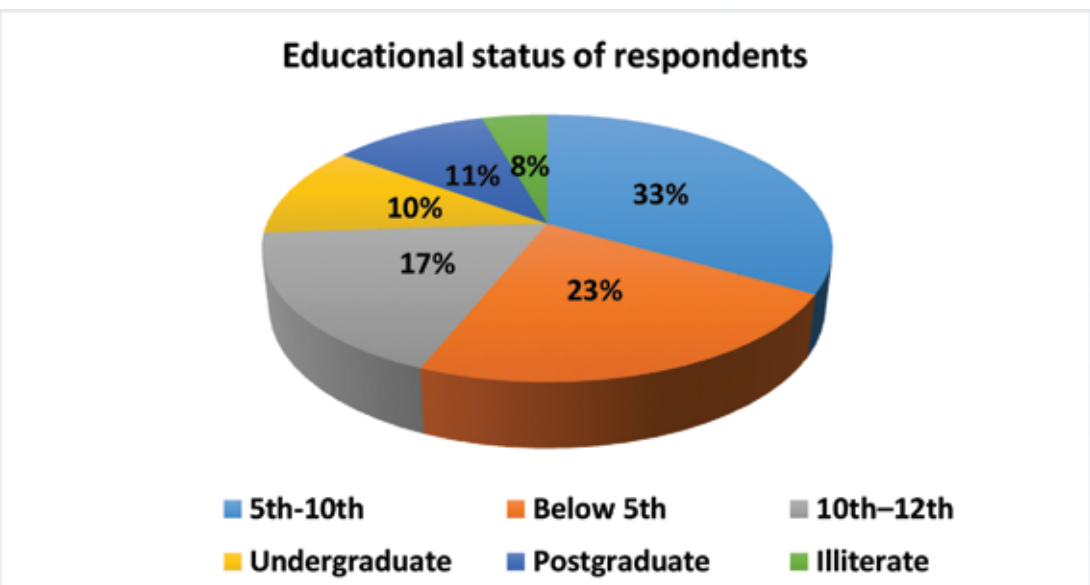



*Figure 44: Respondents educational qualification*

higher education. This highlights a possible gap in digital literacy and awareness of cyber safety practices, as education is closely linked to online safety understanding.

**Adolescentsaged 10-19 years in family**

- The largest segment (34%) of families has two adolescents, showing that siblings in the same age group are common. This could influence peer learning and also shared digital habits.

- Around 31% of families have only one adolescent, indicating that nearly one-third of parents can give exclusive attention to their child's online activities.
- 18% of families have three adolescents, suggesting increased parental responsibility in monitoring multiple children's cyber safety.
- 11% of families have 4–5 adolescents, and 6% have six or more adolescents. While these are smaller groups, they highlight households where parental monitoring is more challenging due to larger family size.

The chart clearly shows that most families (65%) fall in the 1–2 adolescent category, suggesting greater feasibility for parents to engage in close communication and supervision regarding online risks. However, families with 3

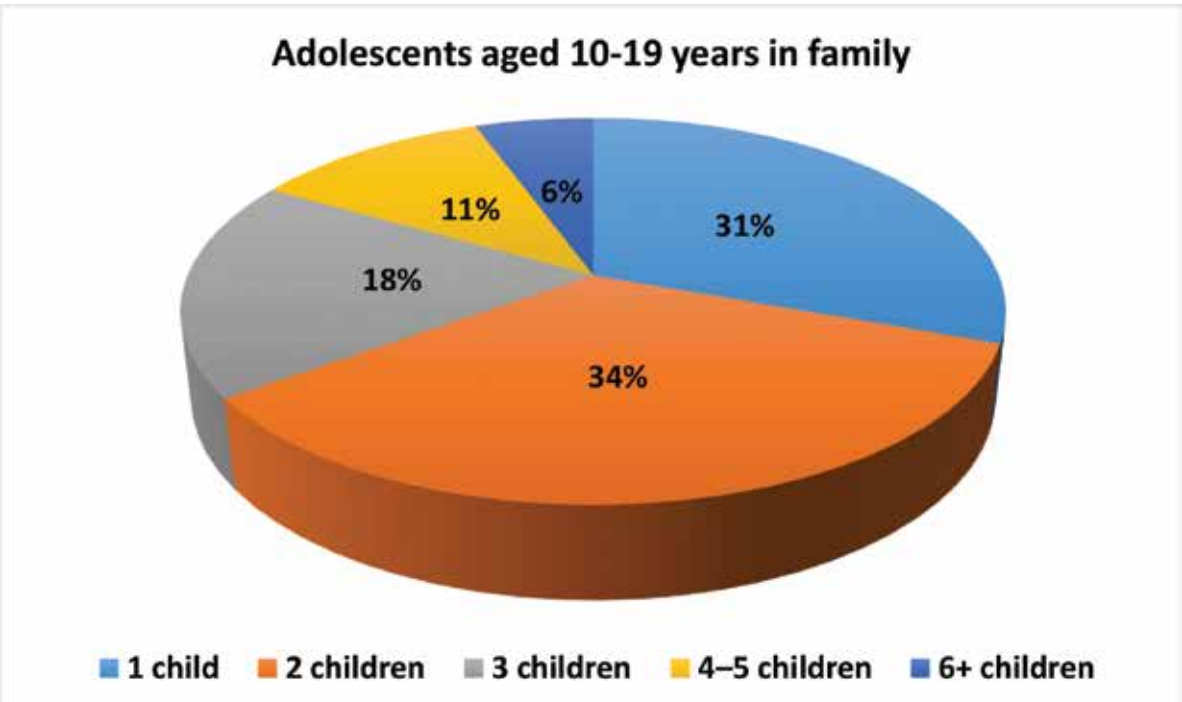


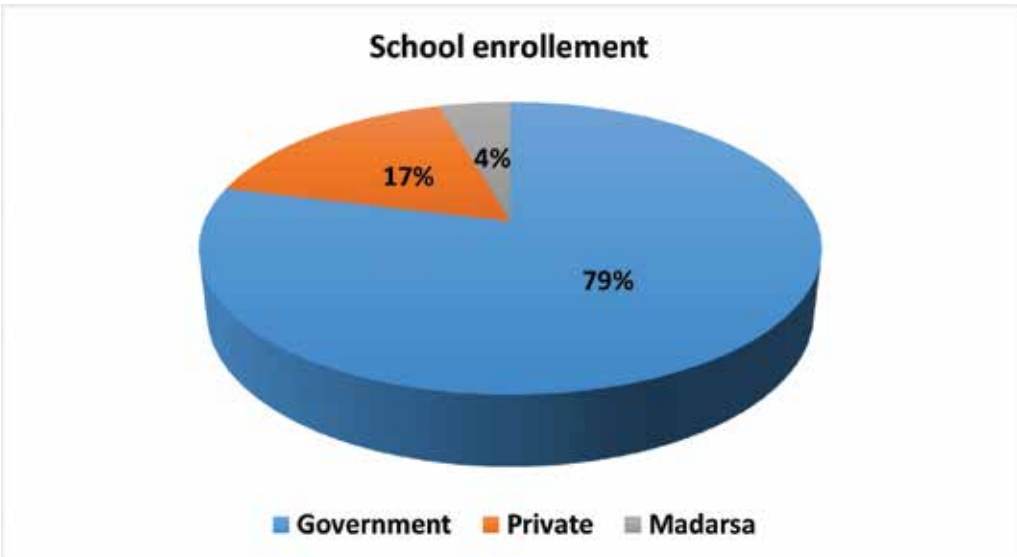

*Figure 45: Number of adolescents in families*

or more adolescents (35%) may face divided attention and less control, potentially exposing children to higher cyber safety risks.

**Type of schools where adolescents are enrolled**

- A significant majority (79%) adolescents are enrolled in government schools, highlighting that public education remains the primary source of schooling for most families. This reflects both affordability and accessibility of government institutions.
- About 17% adolescents'study in private schools, indicating that a smaller but notable proportion of families prefer private education—possibly due to perceived better infrastructure, teaching quality, or focus on English-medium learning.
- A small share (4%) adolescentsis enrolled in Madarsas, which reflects the presence of religious/faith-based education within the community, though it forms only a minor proportion compared to government and private schools.

The chart emphasizes that government schools are the key entry point for implementing large-scale adolescent cyber safety initiatives, while private schools and other religious educational institutions require tailored approaches to ensure inclusivity.




**Online time spent by adolescents**

The chart illustrates the amount of time children spend online on a daily basis. The largest group, 47%, spends 1–3 hours online, which suggests that for nearly half of the children, internet use is a regular but relatively moderate part of their daily routine. Another 27% spend less than 1 hour, indicating limited exposure, possibly due to parental restrictions, academic priorities, or lesser dependence on online activities.

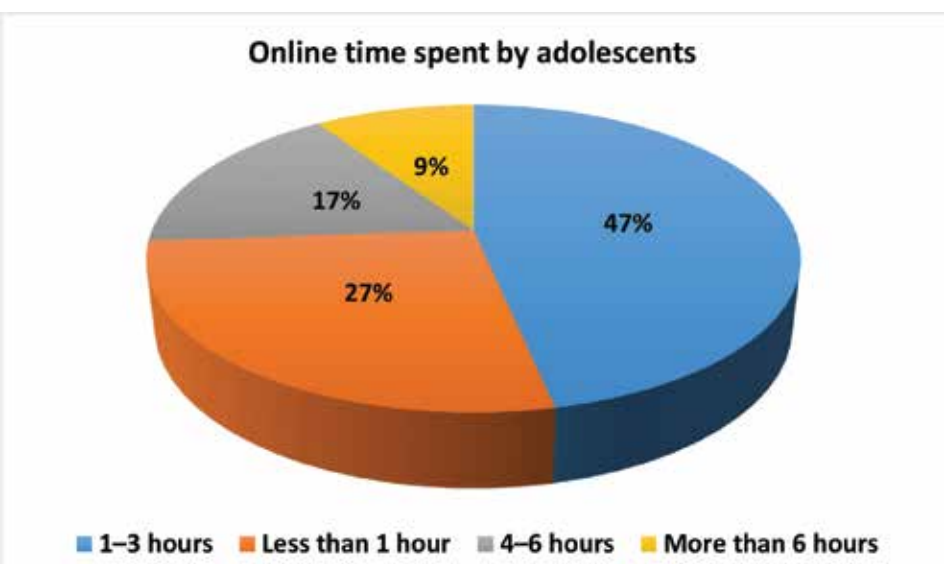



*Figure 46: Time spent by adolescents on internet*

Meanwhile, 17% of children spend 4–6 hours online, reflecting more intensive engagement, which could be linked to extended entertainment use, social media activity, or even online learning. A smaller but still significant 9% spend more than 6 hours online, which highlights a group at potential risk of overexposure, raising concerns about digital addiction, reduced physical activity, and its impact on health and well-being.

The data shows that while the majority of children (74%) fall within a moderate range of online usage (less than 3 hours), there is a considerable proportion (26%) who spend extended periods online, emphasizing the need for balanced screen time management, awareness about healthy digital habits, and parental or school-based guidance.

**Familiarity with concept of cyber safety**

The chart highlights children's familiarity with the concept of cyber safety. A majority, 69%, reported being familiar with cyber safety, suggesting that awareness initiatives, digital exposure, or school-based sensitization have reached a large section of children.

However, 17% of children are not familiar with the concept at all, which indicates a significant knowledge gap that could leave them vulnerable to online risks such as cyberbullying, scams, or privacy breaches. Additionally, 14% of parents are only "somewhat" familiar, reflecting partial understanding that may not be sufficient to ensure safe online practices.

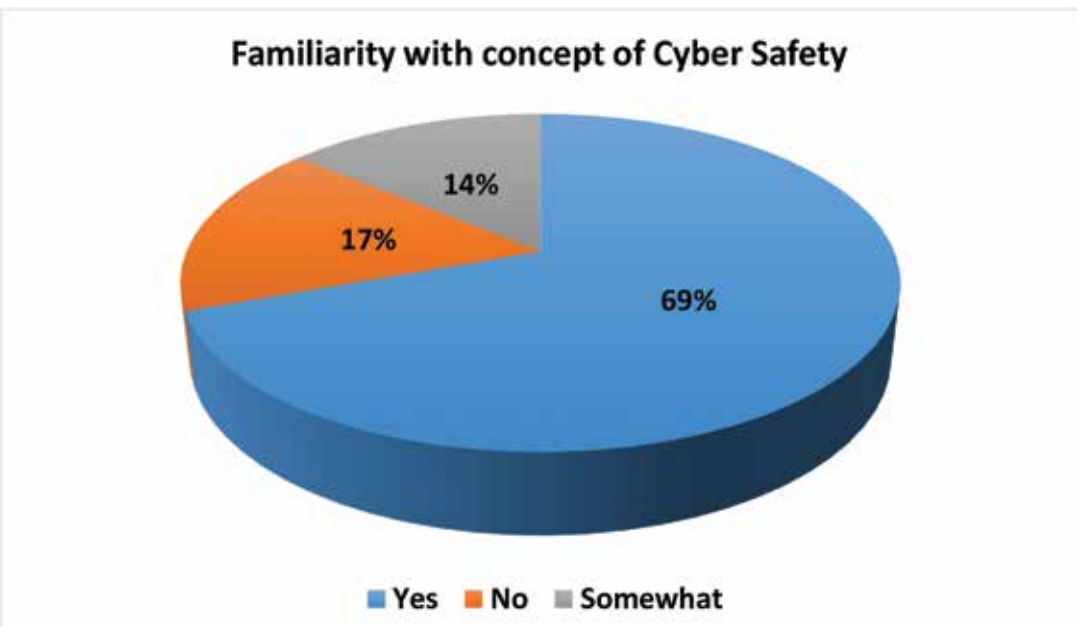



*Figure 47: Parent's familiarity with Cyber Safety*

Overall, while the data is encouraging in showing that most children (nearly 7 in 10) are aware of cyber safety, the combined 31% (No + Somewhat) reveals a critical need for targeted awareness programs, interactive training sessions, and parental involvement to strengthen cyber safety knowledge. Ensuring that all children not only know the concept but can also apply safe practices online will be essential to protecting them in an increasingly digital world.

**Sleeping disorder noticed by parents among their children**

The chart shows parents' observations of sleeping disorders among adolescents. A slight majority, 53% of parents, reported that their children do not have any noticeable sleep-related issues. However, a significant 47% of parents have noticed sleeping disorders in their children.

This near-equal distribution is concerning, as almost half of the children are perceived to be experiencing sleep-related problems. These issues could be linked to excessive screen time, late-night internet or social media use, academic stress, or other lifestyle factors. Sleep disruption in adolescents is known to impact concentration, academic performance, emotional well-being, and overall health.

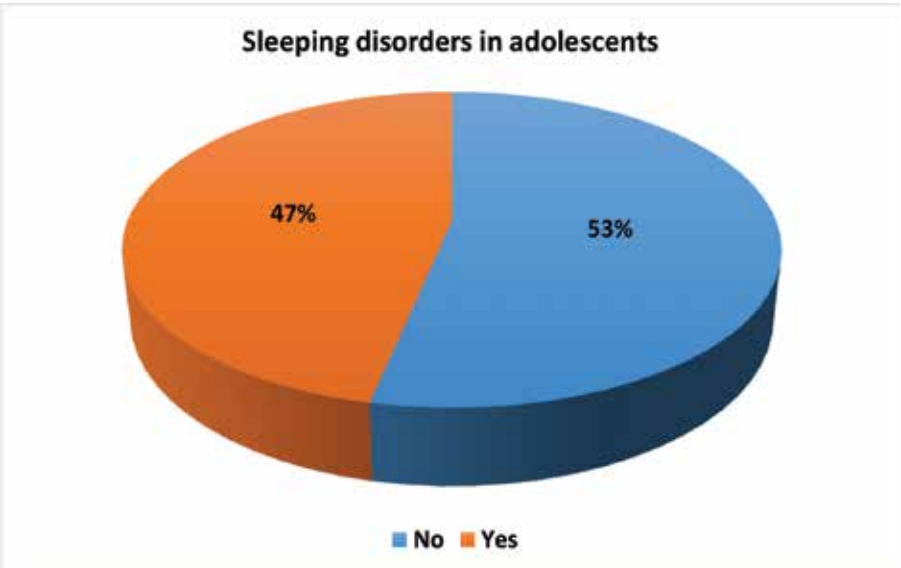



*Figure 48: Sleeping disorders in adolescents*

The data suggests that while some children maintain healthy sleep patterns, a large proportion are at risk of sleep-related challenges. This highlights the urgent need for awareness among parents, digital discipline at home, and counseling support for adolescents, ensuring a balance between online engagement and healthy lifestyle habits.

**Changes in food behavior among adolescents**

The chart illustrates parents' observations regarding changes in food behavior among adolescents. A slight majority, 54% of parents, reported no noticeable change in their children's eating patterns, while a significant 46% observed changes in food behavior.

The fact that nearly half of the parents noticed changes is noteworthy, as it may point to underlying influences such as increased screen time, stress, irregular routines, or exposure to digital advertisements promoting unhealthy food choices. These behavioral shifts could manifest as skipping meals, preference for junk food, overeating, or reduced appetite—all of which can affect adolescents' nutrition and overall health.

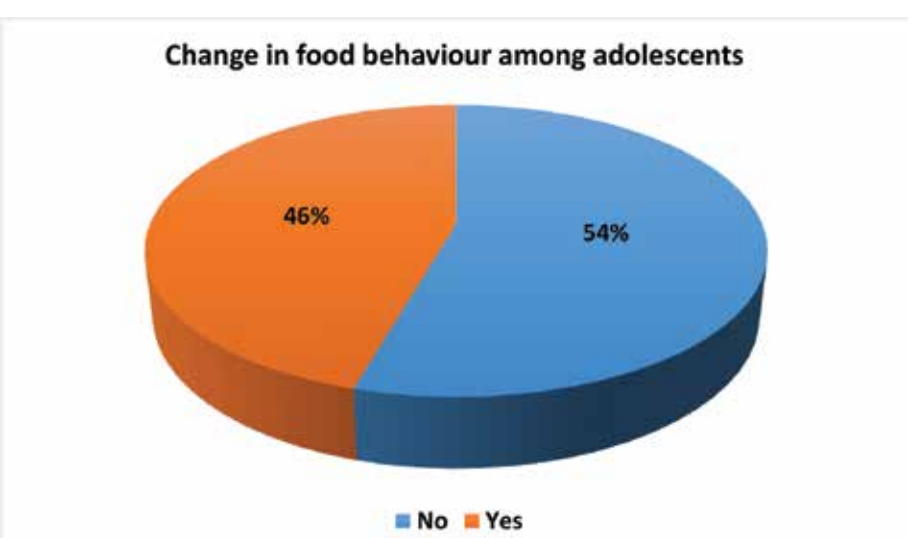



*Figure 49: Food behavior among adolescents*

Overall, the data suggests that while a majority of adolescents maintain stable eating habits, a large portion are experiencing disruptions. This highlights the importance of parental guidance, balanced routines, and awareness programs on healthy lifestyle choices, ensuring that digital engagement does not negatively impact adolescents' dietary behavior.

**Monitoring child's online activities**

The chart illustrates how parents monitor their children's online activities. A significant share, 39% of parents, reported monitoring their child's activities regularly, which reflects proactive involvement in ensuring online safety. Meanwhile, 30% monitor rarely, suggesting a more relaxed approach where digital supervision is occasional rather than consistent.

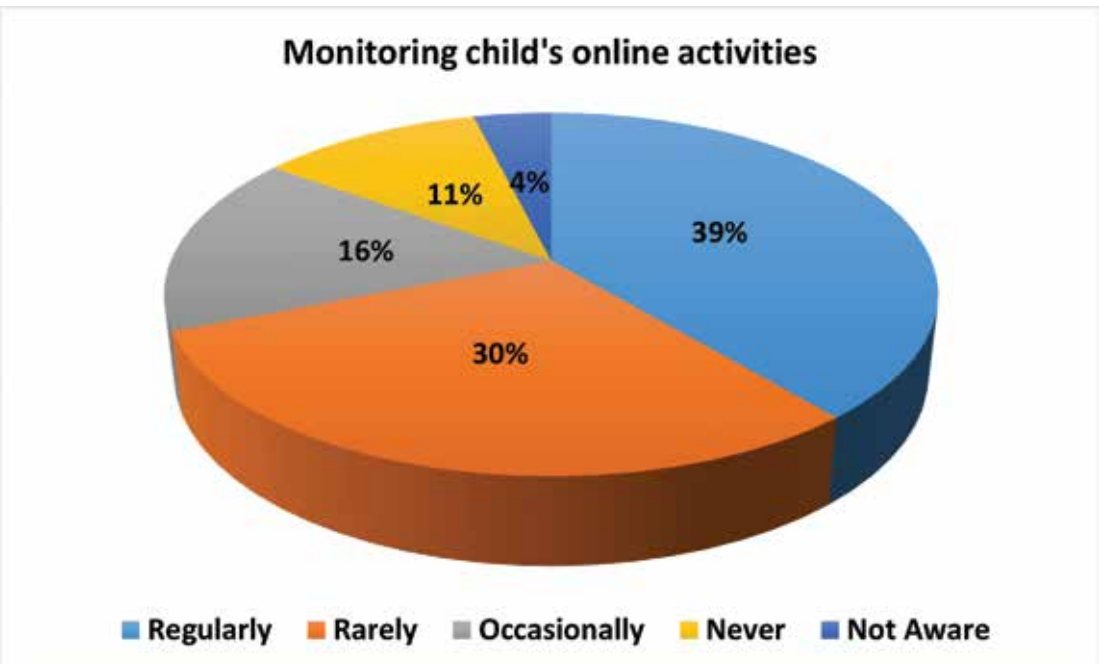



*Figure 50: Monitoring of online activities*

Additionally, 16% of parents monitor occasionally, indicating periodic checks without routine vigilance, while 11% reported never monitoring their child's online activities—leaving children largely unsupervised in the digital space. A smaller group, 4%, stated they are not aware of their child's online engagements, highlighting a lack of connection with their child's internet usage.

Overall, the data shows that while a majority of parents (85% combining regularly, rarely, and occasionally) are at least somewhat engaged in monitoring, there remains a considerable group (15%) that either never monitors or is unaware. This gap underlines the need for awareness programs and parental digital literacy initiatives to strengthen parents' capacity to guide and safeguard adolescents in the online environment.

**Parental control tool used by parents**

The chart illustrates the use of parental control tools by parents to regulate their children's online activities. A majority, 58% of parents, reported that they do not use any such tools, indicating a heavy reliance on personal monitoring or trust in their child's online behavior rather than technological support. Meanwhile, 22% of parents are not even aware of these tools, highlighting a significant knowledge gap in digital parenting practices. Only 20% of parents actively use parental control tools, reflecting a relatively small proportion who adopt technology-based solutions to ensure cyber safety.

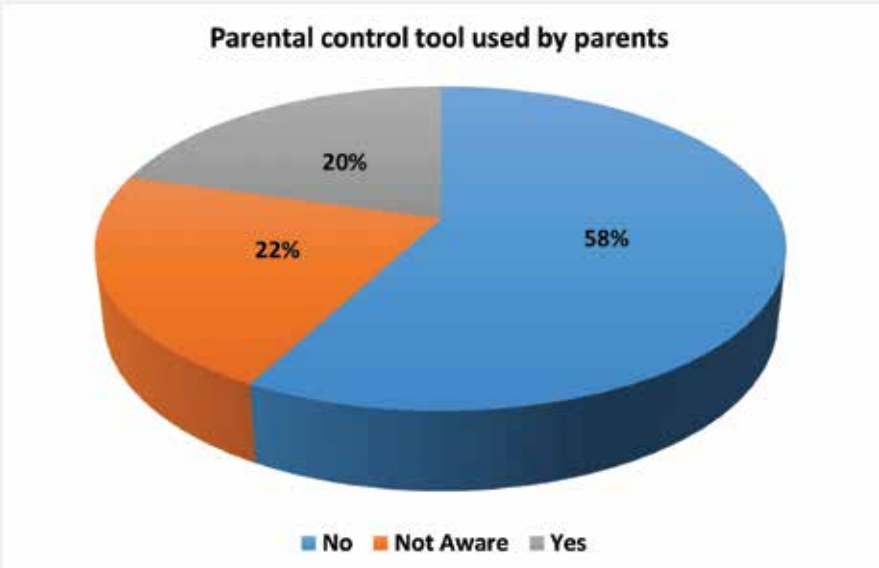



*Figure 51: Use of parental control tool*

This data suggests that while most parents are concerned about their children's online exposure (as seen in monitoring patterns), the actual adoption of specialized control tools remains low. Lack of awareness and limited digital literacy among parents may be key barriers. The findings highlight the need for capacity-building programs, awareness campaigns, and demonstrations of parental control applications to empower parents with effective strategies for safeguarding their children online. By bridging this knowledge and usage gap, parents can play a more proactive role in ensuring safer digital environments for adolescents.

**Level of interaction between parents and children about online safety**

The chart reflects the level of interaction between parents and children about online safety. The largest share, 32% of parents, interact rarely, indicating that discussions about safe internet use are infrequent in many households. Meanwhile, 27% sometimes discuss online safety, and another 27% regularly engage in such conversations, reflecting a more balanced parental involvement. However, 14% of parents never discuss online safety with their children, leaving a significant portion of adolescents without essential guidance in navigating the digital world.

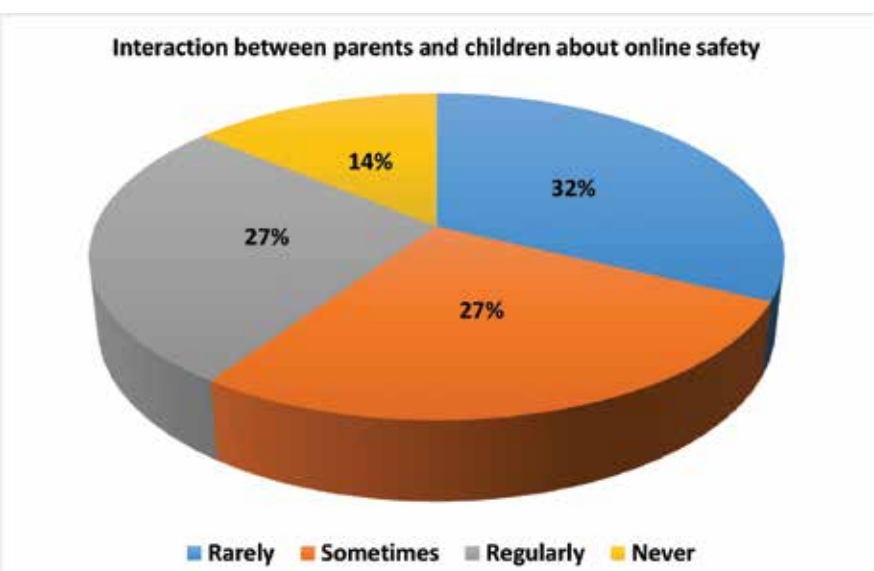



*Figure 52: Parents-children interaction on online safety*

Overall, the findings highlight a mixed picture—while more than half of parents (54%) engage at least sometimes or regularly in conversations about online safety, a considerable share either rarely do so or not at all. This gap suggests the need for greater sensitization of parents on the importance of open, consistent dialogue with children regarding online risks, digital etiquette, and safe practices. Encouraging structured and ongoing communication can build trust and equip adolescents to handle challenges in the digital environment more confidently and responsibly.

**Parental-Child communication on sharing online threats**

The chart highlights the relationship between parents and children regarding the sharing of online threats faced by adolescents. Nearly half, 49% of parents, believe that their children feel comfortable sharing online threats with them. This is a positive sign, suggesting that many families have established trust and open communication channels. However, 23% of parents responded with “Maybe,” indicating uncertainty about whether their children would actually confide in them, which reflects possible gaps in communication or trust.

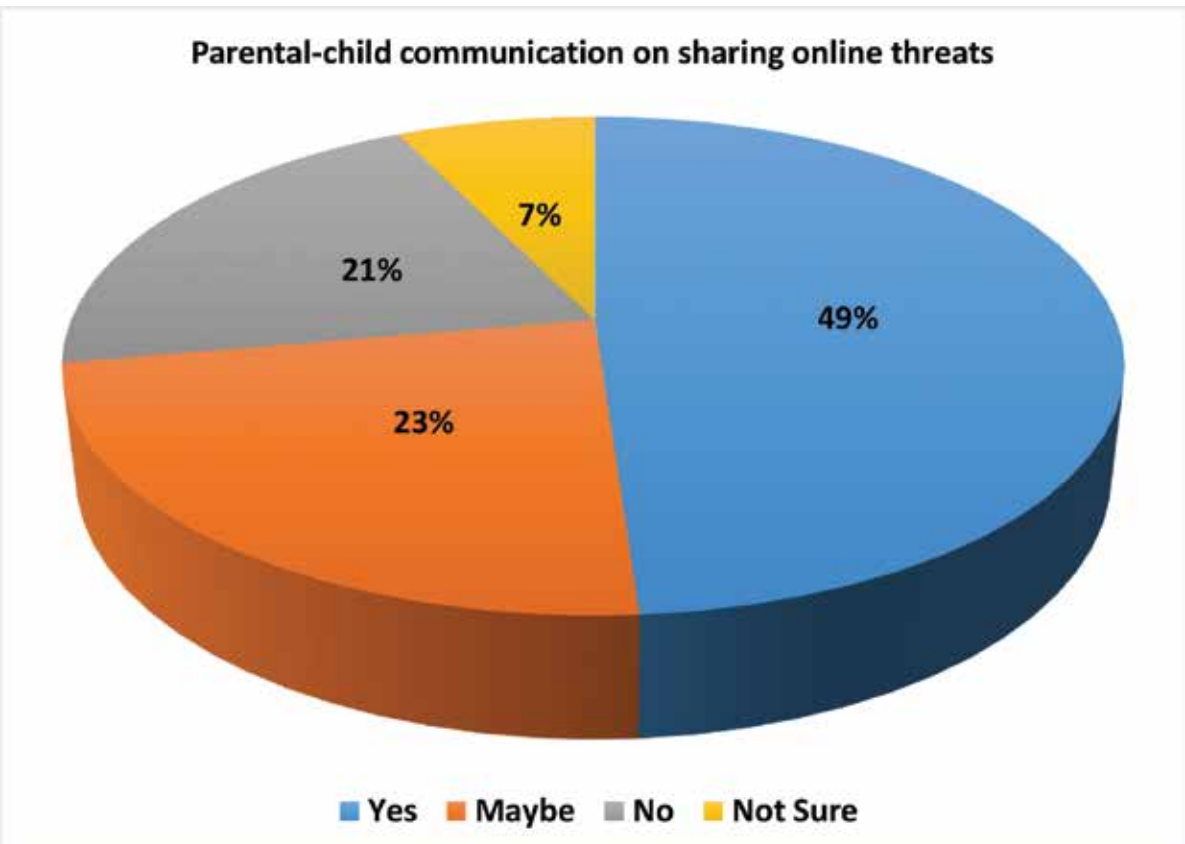



*Figure 53: Parents-child interaction online threats*

At the same time, 21% of parents acknowledged that their children do not share online threats, pointing to a significant proportion of adolescents who may be dealing with digital risks in silence. Furthermore, 7% of parents are not sure, highlighting a lack of awareness about their child’s behavior or level of openness in this context.

Overall, while nearly half of the families demonstrate strong communication on online safety issues, the other half reflect uncertainty, reluctance, or disengagement. This underlines the need for awareness programs that encourage stronger parent-child dialogue, promote trust-building, and help parents create safe spaces for adolescents to openly discuss the online challenges they face.

**School-based initiatives on cyber safety awareness**

The chart shows parents' perspectives on whether cyber safety sessions are conducted by schools. Nearly half, 48%, confirmed that such sessions have been organized, indicating that schools are playing an active role in educating children about safe online practices. However, a significant 30% of parents reported that no such sessions were conducted, pointing to gaps in school-based digital literacy initiatives.

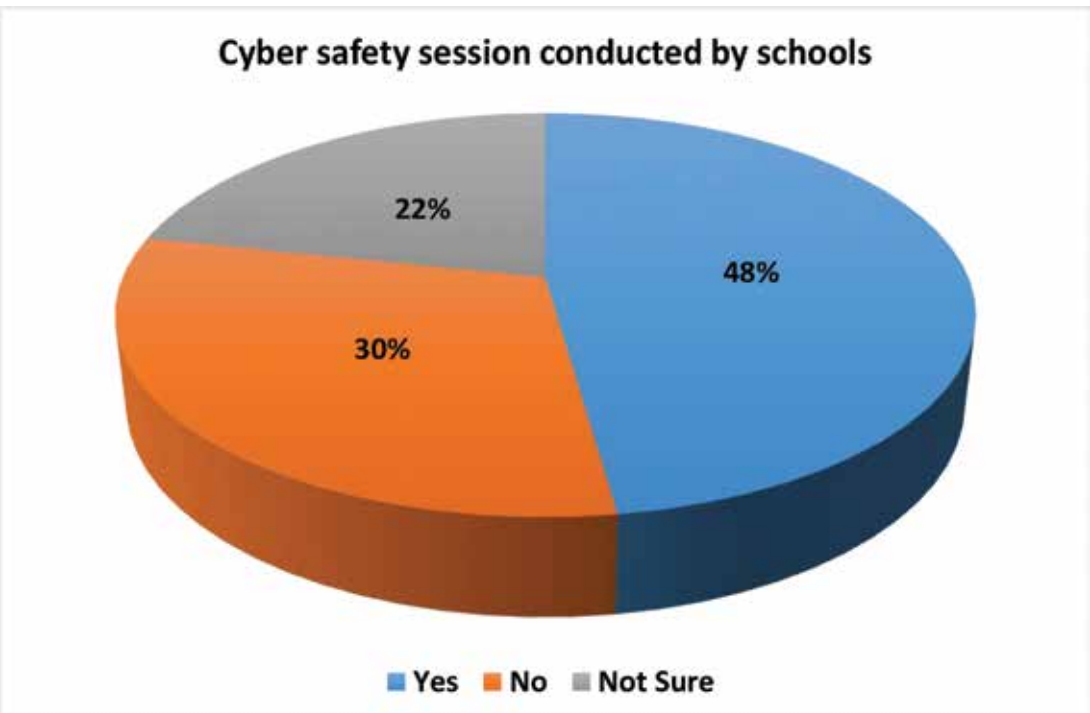



*Figure 54: Cyber safety sessions conducted by schools*

Additionally, 22% of parents were not sure whether cyber safety sessions had been held, which could reflect either limited communication from schools or lack of parental engagement with school activities.

Overall, while it is encouraging that many schools have taken steps to address cyber safety, the data reveals that over half of parents (52%) are either unaware or state that schools have not conducted such sessions. This highlights the need for consistent, structured, and visible cyber safety programs in schools, alongwith better communication to parents, ensuring that both children and families are equipped to navigate digital risks effectively.

The chart presents the biggest online threats to adolescents as perceived by respondents, categorized into major risk areas. The largest concern, identified by 23%, is excessive phone/internet use and addiction, showing widespread worry about overdependence on devices and its impact on adolescents' lifestyle and mental well-being. Following this, 20% pointed to social media risks such as fake identities, interaction with strangers, misuse of reels, and unsafe platforms, reflecting concerns about unsafe online interactions.

Another 16% highlighted online frauds and scams, including OTP frauds, financial scams, hacking, and blackmailing, indicating fears around exploitation and online financial risks. Similarly, 11% of respondents noted privacy and security risks, including data theft, sharing of real photos, and exposure to inappropriate content. In addition, 9% raised concerns about health and behavioral issues, such as sleep disturbances, eye problems, and distraction from studies, showing the offline impact of digital habits.

Interestingly, 18% of respondents reported “no threat”, suggesting either a lack of awareness of online dangers or a belief that their children are safe. While this perception may reflect confidence in parental supervision, it also signals potential underestimation of real risks.

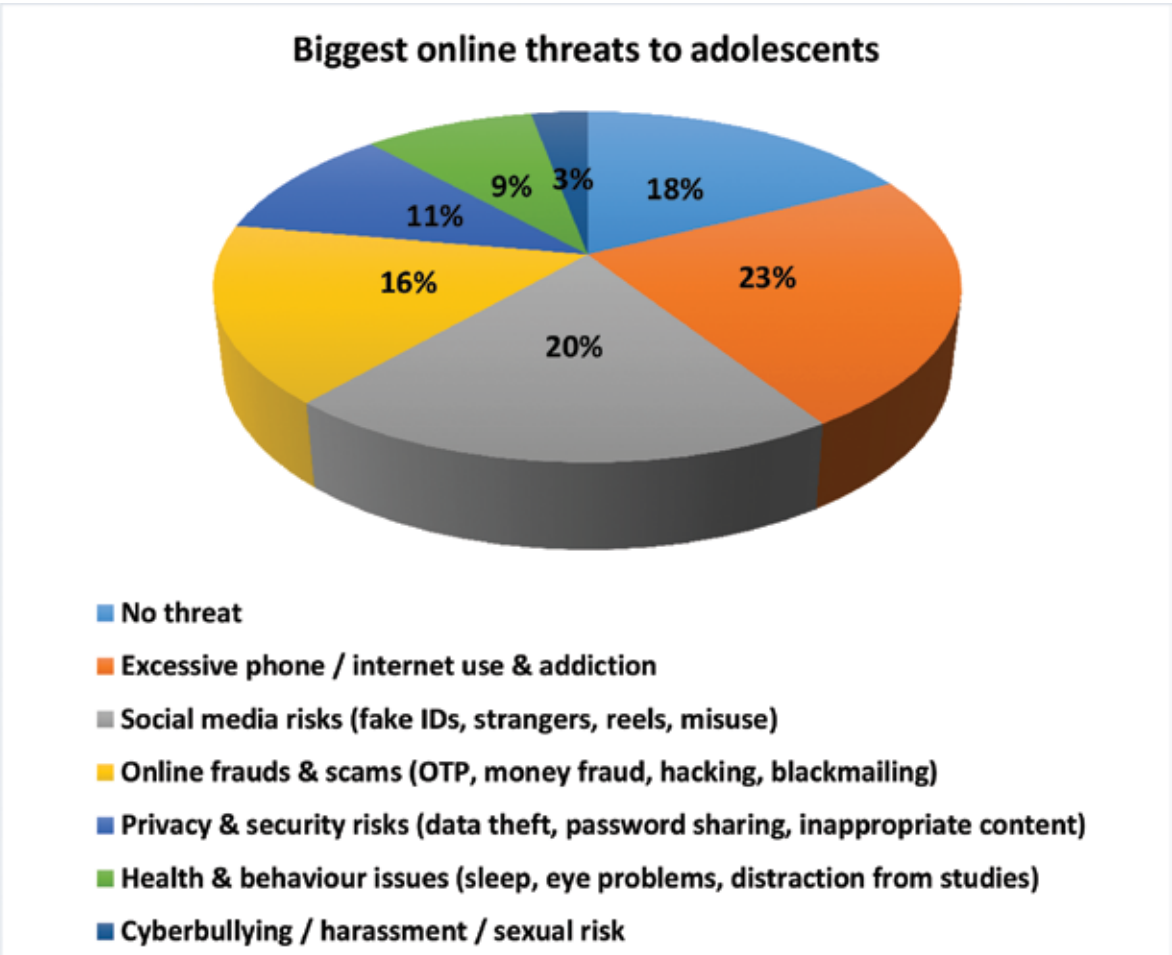



*Figure 55: Biggest online threats to adolescents*

The analysis of parents’ suggestions for schools on cyber safety shows some clear trends. About one-fourth (24%) of parents emphasized the need for regular awareness sessions—whether monthly, teacher-led, or through workshops—to better prepare children for online risks. Similarly, around 22% suggested banning or restricting mobile phones in schools and avoiding phone-based homework, reflecting strong concerns about misuse of devices in academic settings. Another 14% highlighted the role of parents and teachers working together through joint sessions, counselling, and guidance, showing the importance of collective responsibility in digital safety. About 8% recommended including cyber safety in the school curriculum, with a focus on ethical technology use and digital literacy. A smaller group, 5% of parents, suggested practical measures such as self-defence training, monitoring apps, and helplines. Interestingly, the largest share, 27%, either gave no suggestions or were unsure, which points to a gap in parental awareness. Overall, the findings show that parents strongly expect schools to play a proactive role in cyber safety education while also limiting digital exposure within school environments.

**Parental suggestions for strengthening cyber safety**

The analysis of parents’ suggestions for schools on cyber safety shows some clear trends. About one-fourth (24%) of parents emphasized the need for regular awareness sessions—whether monthly, teacher-led, or through workshops—to better prepare children for online risks.

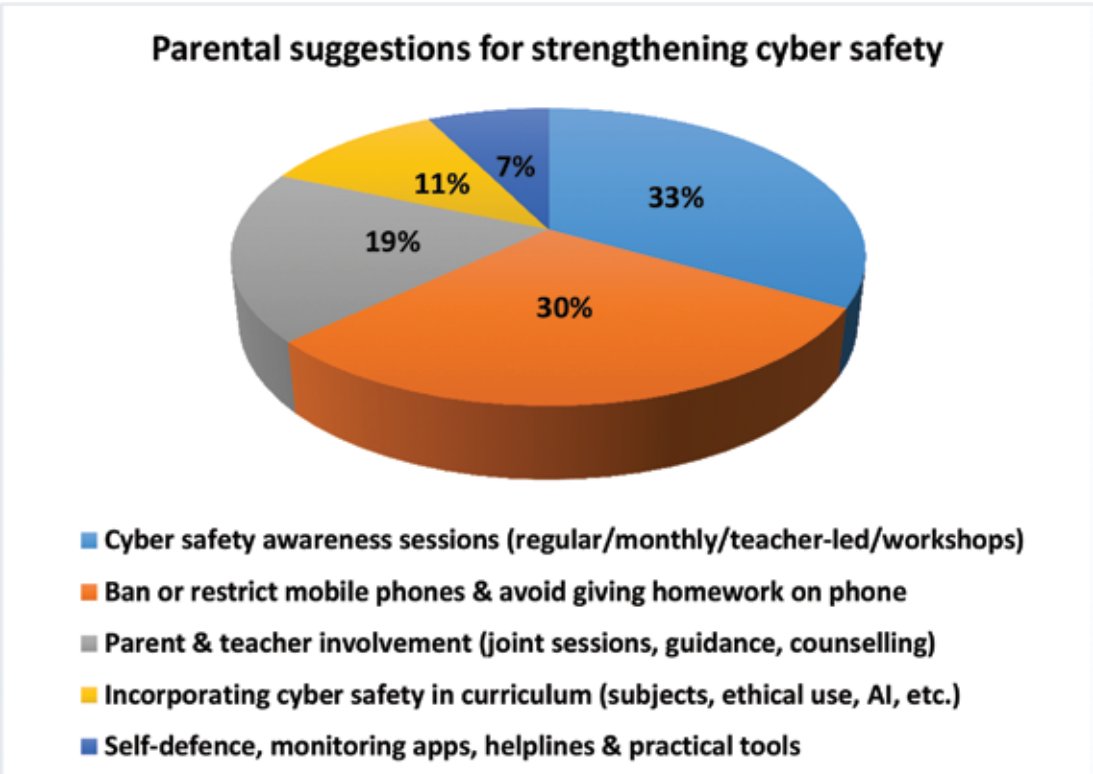



*Figure 56: Parent's suggestions on cyber safety*

Similarly, around 22% suggested banning or restricting mobile phones in schools and avoiding phone-based homework, reflecting strong concerns about misuse of devices in academic settings. Another 14% highlighted the role of parents and teachers working together through joint sessions, counselling, and guidance, showing the importance of collective responsibility in digital safety.

About 8% recommended including cyber safety in the school curriculum, with a focus on ethical technology use and digital literacy. A smaller group, 5% of parents, suggested practical measures such as self-defense training, monitoring apps, and helplines. Interestingly, the largest share, 27%, either gave no suggestions or were unsure, which points to a gap in parental awareness. Overall, the findings show that parents strongly expect schools to play a proactive role in cyber safety education while also limiting digital exposure within school environments.

# School Authorities' Encounters and Role in Digital Safety

# Chapter10: School Authorities' Encounters and Role in Digital Safety

**Schools' coverage in the study**

The chart shows that most schools covered in the study are government institutions(89%), while only 11% are private. This means the findings mainly reflect how government schools perceive and implement cyber safety, where challenges like limited resources and lack of specialized staff remain critical.

The underrepresentation of private schools leaves a gap, as they often have higher digital exposure through device ownership and social media use. Therefore, while government schools need continued focus on awareness and training, private schools must also be systematically engaged to ensure all adolescents are equally protected in the digital space.

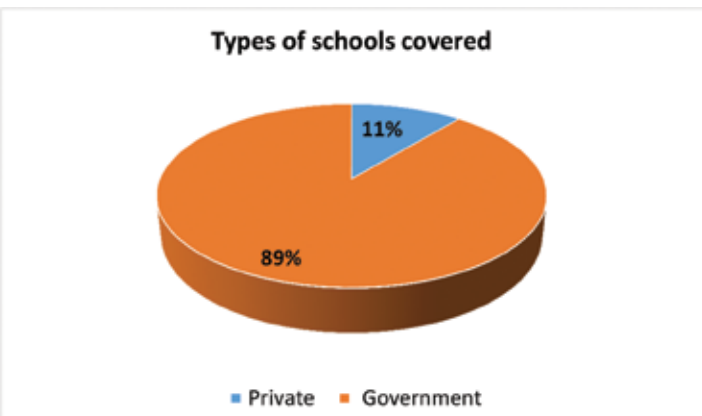



*Figure 57: Type of schools covered*

**Respondents profile**

The chart shows that the majority of respondents in the study are teachers (72%), while principals account for 28%. This suggests that the perspectives captured lean heavily toward classroom-level experiences, where teachers interact directly with students and witness their day-to-day digital behaviors and challenges.

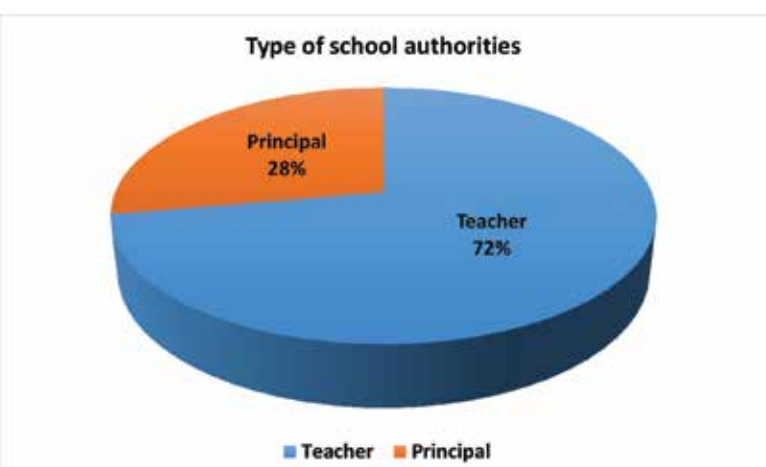



*Figure 58: Type of school authorities*

Their inputs are valuable for understanding practical issues of implementation, such as managing screen time, addressing cyberbullying, or integrating cyber safety discussions into teaching. However, principals, as the policy and decision-making heads of schools, are underrepresented, which creates a gap in reflecting on institutional-level strategies and policy enforcement.

Taken together, the data indicates that while teachers' voices provide important ground realities, a stronger representation of principals is needed to balance operational experiences with leadership perspectives for a comprehensive view of cyber safety readiness in schools.

**Experience in Field of Education**

The chart on "Experience in Field of Education" highlights that 33% of respondents have more than 20 years of experience, followed by 28% with 11–20 years, 22% with less than 5 years, and 17% with 5–10 years.

This distribution shows that the study is enriched with perspectives from highly experienced school authorities who bring long-term institutional knowledge and policy-level insights. At the same time, a considerable share of mid-career and early-career educators contributes viewpoints that reflect the contemporary realities of adolescents' digital engagement.

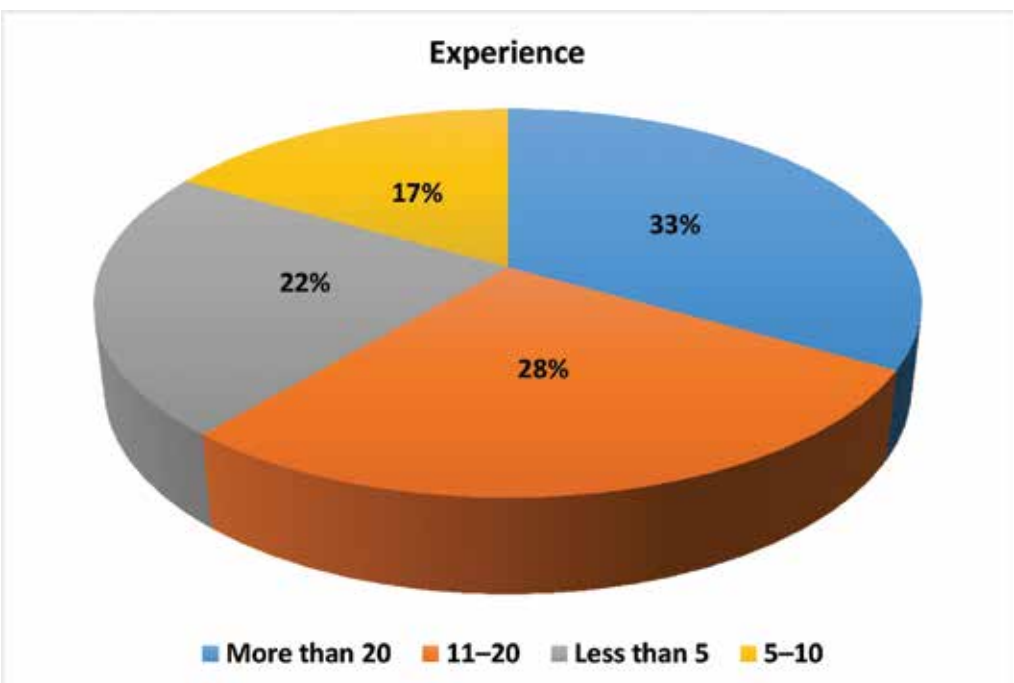



*Figure 59: Educational experience*

The mix of seniority levels ensures that the findings capture both the strategic oversight of veteran educators and the practical classroom experiences of newer staff, making the understanding of cyber safety challenges and practices more balanced and comprehensive.

**Schools with internet facilities**

The chart shows that 100% of the schools surveyed have internet access. This finding is significant because it indicates that all participating schools are digitally connected, which is essential for modern teaching, administration, and student learning.

However, while universal internet availability creates opportunities for digital education, it also increases exposure to cyber risks such as online bullying, scams, and unsafe content. From the perspective of school authorities, this

reinforces the urgency of implementing cyber safety policies, staff training, and awareness programs to ensure that the benefits of internet access are maximized while minimizing potential harms. In short, the presence of internet facilities in all schools provides a strong foundation for digital education, but it also makes cyber safety preparedness a non-negotiable priority.

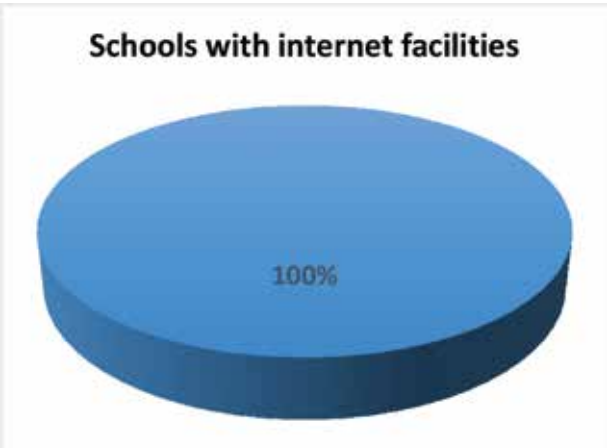



*Figure 60: Internet facilities in schools*

**Internet access for teaching staff**

The chart shows that 100% of teachers in the surveyed schools have access to the internet. This is an encouraging sign, as it ensures that educators are equipped to use digital tools for teaching, accessing resources, and guiding students in the online space. However, universal access also means that teachers themselves must be adequately trained in cyber safety practices, since they play a frontline role in modeling safe online behavior and in guiding adolescents.

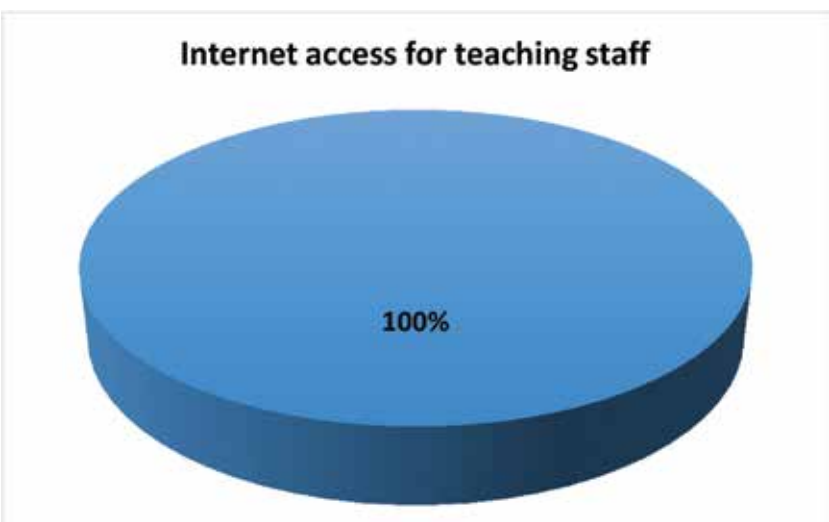



*Figure 61: Internet access for teaching staff*

**Permission to Bring Personal Phone/Tablet**

The chart shows that a majority of schools (55%) do not allow students to bring personal devices, while 28% permit them with restrictions and 17% allow them freely. This indicates that most school authorities recognize the risks associated with unrestricted device use, such as exposure to inappropriate content, distraction in classrooms, and cyberbullying.

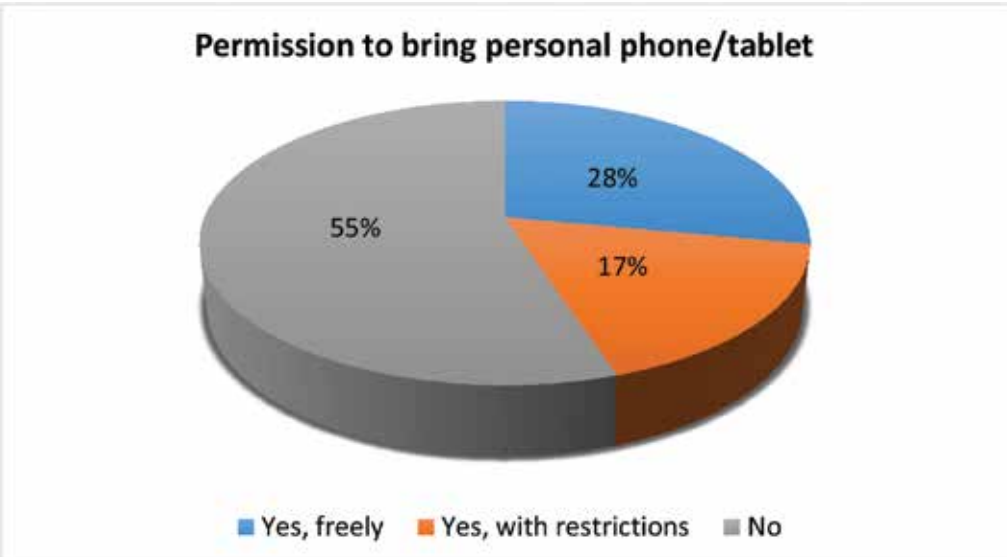



*Figure 62: Use of mobile phones and tablets in schools*

However, the fact that nearly half of the schools (45%) still permit personal devices—whether restricted or freely—highlights a balancing act between enabling digital access and maintaining discipline. Schools that impose restrictions are likely attempting to integrate technology for learning while keeping safeguards in place.

On the other hand, those allowing free use may face greater challenges in monitoring online behavior. Overall, the findings underscore the need for clear policies, digital literacy programs, and robust monitoring mechanisms to ensure that personal devices, when allowed, support learning without compromising cyber safety.

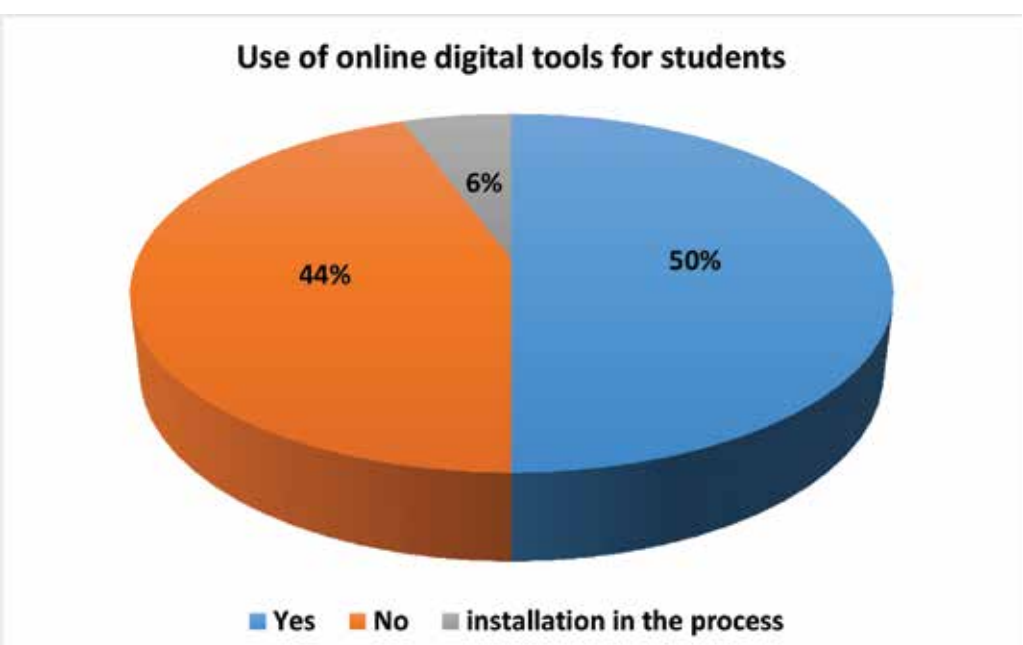



*Figure 63: Online educational tools for students*

**Use of online digital tools for students**

The chart shows that 50% of schools are already using digital tools, 44% are not, and 6% are in the process of installing them. This reflects a growing but uneven adoption of technology in classrooms. Schools that have integrated digital tools are likely better positioned to enhance learning and promote safe digital practices, but

the significant proportion of schools not using them points to a digital gap that may limit students' exposure to structured online learning.

The small group currently in transition indicates a positive trend, suggesting that more schools are moving toward digitization. From a cyber safety perspective, this uneven adoption means that while some students are gaining both digital opportunities and risks, others remain outside the digital ecosystem, potentially contributing to disparities in preparedness for safe online engagement.

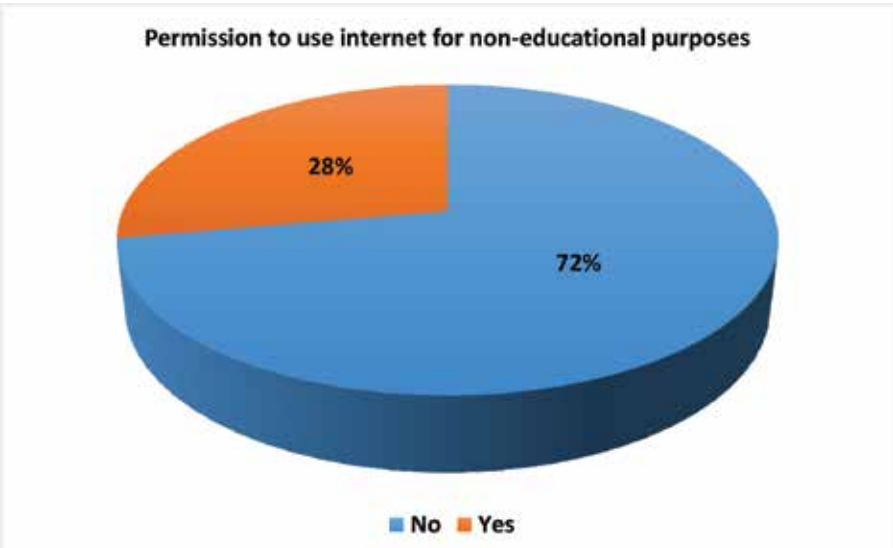



*Figure 64: Internet for non-educational purposes*

**Permission to use internet for non-educational purposes**

The chart shows that 72% of schools do not allow students to access the internet for non-educational activities, while 28% permit it. This indicates that the majority of school authorities are cautious and enforce restrictions to ensure the internet is used primarily for learning, reducing the chances of distractions, misuse, or exposure to unsafe content.

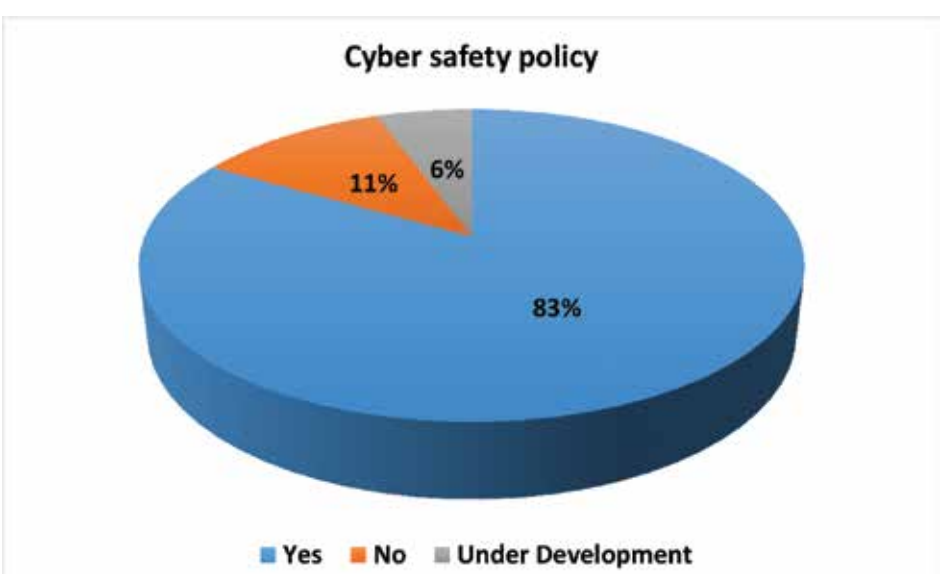



*Figure 65: Cyber safety policy in schools*

However, the fact that over a quarter of schools still allow such use suggests that some institutions may adopt a more flexible approach, possibly to encourage digital exploration or trust-based learning. From a cyber safety perspective, this flexibility can increase risks if not paired with proper monitoring and guidance. Overall, the data reflects a strong emphasis on controlled and education-focused internet use, but it also points to the need for schools to establish clear policies and digital literacy programs so that even non-educational internet use can be managed safely.

**Cyber safety policy in Schools**

The chart shows that 83% of schools have a cyber safety policy in place, 11% do not, and 6% are in the process of developing one. This is a highly encouraging finding, as it indicates that the majority of schools have recognized the importance of structured policies to safeguard adolescents in the digital space.

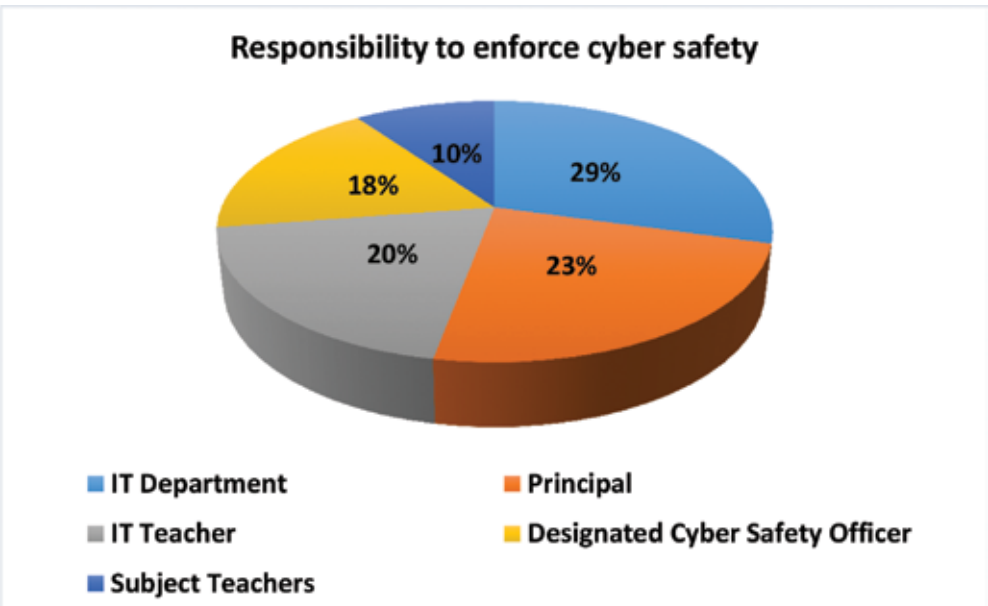



*Figure 66: Responsibility to enforce cyber safety in schools*

The presence of such policies reflects alignment with the NCPCR/NCERT guidelines, which emphasize integrating cyber safety into school codes of conduct, training, and reporting mechanisms. However, the 11% without a policy highlights a concerning gap, as these schools leave students more vulnerable to online risks without formal protective measures.

The small share of schools with policies under development (6%) shows progress, but also suggests that some institutions are still in the early stages of formalizing their approach. Overall, the data underscores that while policy adoption is widespread, the next challenge lies in effective implementation, staff training, and consistent monitoring to ensure these policies translate into safe digital environments for students.

**Responsibility to enforce cyber safety**

The chart highlights how schools distribute accountability among different stakeholders. The IT Department (29%) is most frequently seen as responsible, followed by the principal (23%), IT teachers (20%), designated cyber safety officers (18%), and subject teachers (10%). This distribution shows that while technical staff (IT Department and IT Teachers) play a leading role, principals continue to be central in ensuring policy-level enforcement.

The inclusion of designated cyber safety officers in nearly one-fifth of cases is an encouraging sign, reflecting alignment with NCPCR/NCPCR guidelines that recommend specialized responsibility. However, the relatively

smaller role of subject teachers suggests that cyber safety is still not fully integrated into everyday classroom teaching.

**Awareness about cyber safety policy**

The chart shows that 93% of school authorities are aware of the existence of a cyber safety policy, while only 7% are not. This is a highly positive indicator, reflecting that the majority of respondents are informed about structured guidelines and frameworks aimed at protecting students in the digital environment. Such high awareness also suggests that schools are aligning themselves with the NCPCR/NCERT directives , which mandate the integration of cyber safety measures into school functioning.

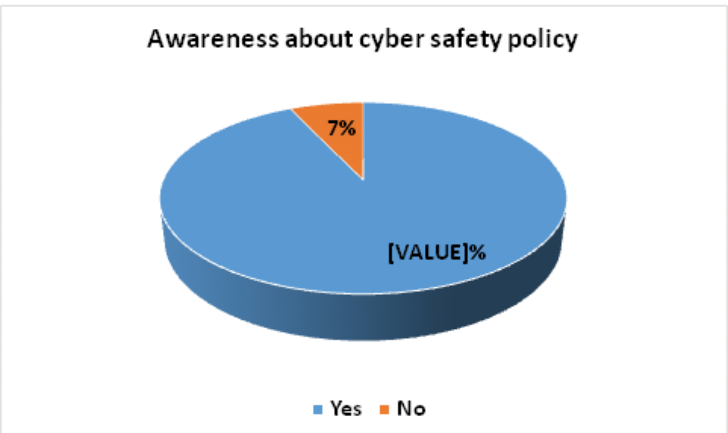



*Figure 67: Awareness about cyber safety policy in schools*

However, the small proportion (7%) of respondents unaware of such policies is still noteworthy, as it points to a communication and sensitization gap within certain institutions. Even if policies exist at the school level, lack of awareness among key stakeholders can weaken their implementation. Overall, the findings highlight that while awareness is strong, schools must ensure consistent dissemination, orientation, and training so that every authority—whether principal, teacher, or IT staff—fully understands and applies the policy in practice.

**Cyber safety guidelines implementation**

The chart revels that **61% of schools have implemented the guidelines, while 39% have not.** This indicates that although a majority of institutions are taking steps to comply with the NCPCR/NCERT directives, a substantial proportion is still lagging behind. The gap suggests that while awareness of policies is high (as seen in the earlier chart), actual enforcement and operationalization remain inconsistent.

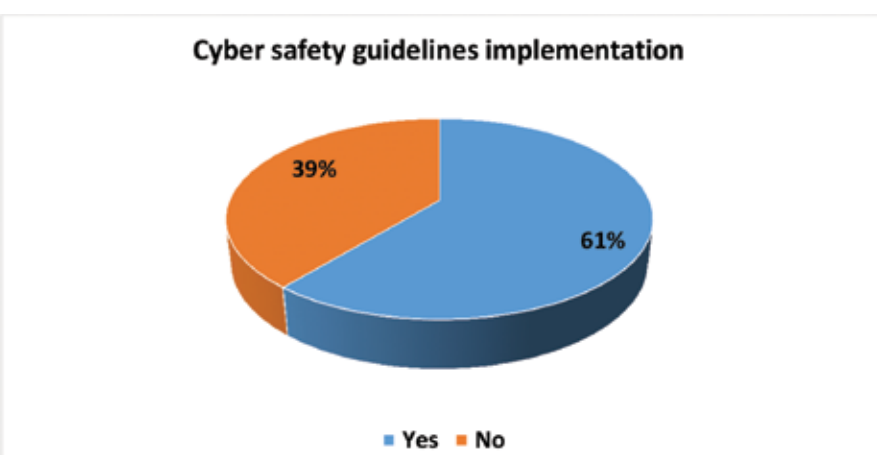



*Figure 68: Implementation of cyber safety guidelines in schools*

The reasons for non-implementation could include lack of trained staff, resource constraints, or weak monitoring mechanisms within schools. This is significant because without proper implementation, even well-designed policies and guidelines cannot protect adolescents from digital risks such as cyberbullying, scams, or exposure to harmful content. The findings highlight that schools need capacity building, technical support, and stronger accountability frameworks to bridge the gap between policy and practice.

**Cyber-safety session for students**

The chart shows that 67% of schools have already conducted sessions, 16% have sessions planned, while 17% have not conducted any. This indicates that most schools recognize the importance of engaging students directly in discussions about online safety, reflecting a proactive step towards awareness and prevention.

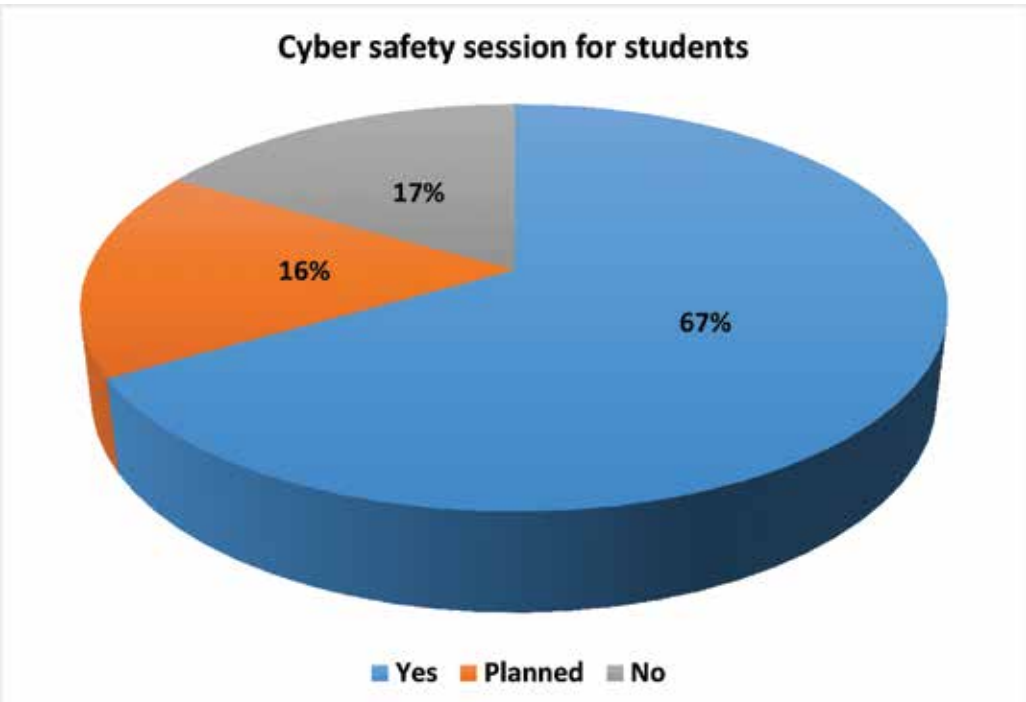



*Figure 69: Cyber safety session for students*

The share of schools with planned sessions suggests positive momentum, showing that more institutions are preparing to integrate such initiatives into their activities.

However, the 17% of schools not conducting sessions points to a gap, as adolescents in these institutions may remain less informed about risks such as cyberbullying, scams, and misuse of personal information. Since students are the most active users of digital platforms, regular cyber safety sessions are critical for equipping them with the knowledge and skills to navigate online spaces safely.

**Cyber-safety workshops for Parents**

The chart shows that 33% of schools have organized workshops for parents, 22% plan to conduct them, while a significant 45% have not conducted any. This highlights a mixed picture of parental engagement in cyber safety. On the positive side, one-third of schools are already involving parents, recognizing their crucial role in guiding children's online behavior at home. The planned workshops further suggest that more schools are beginning to acknowledge the importance of parental sensitization.

However, the fact that nearly half of the schools have not held such workshops indicates a major gap, since **parental awareness and involvement are key to reinforcing safe digital practices outside school boundaries.** Without equipping

parents, efforts at the school level may remain incomplete, as children spend much of their online time outside the classroom.

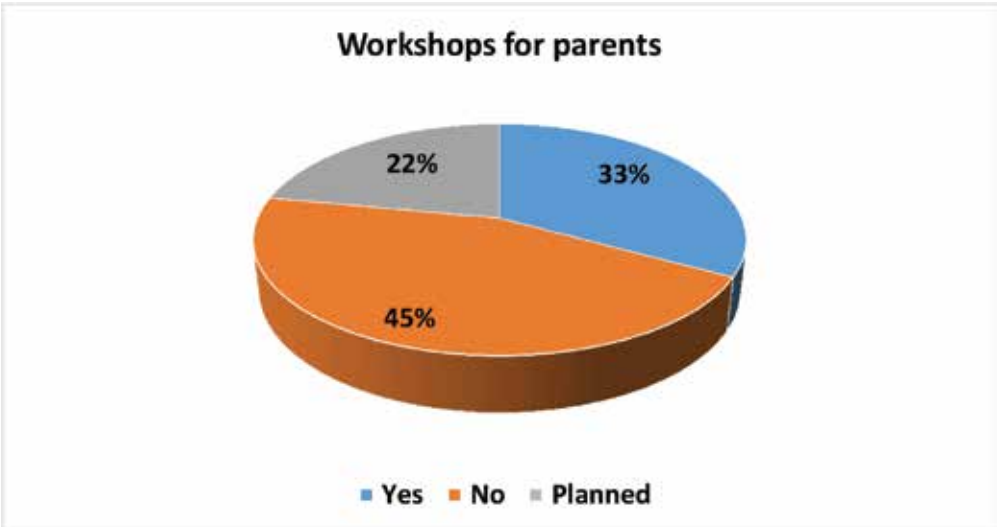



*Figure 70: Cyber safety workshop for parents*

**Status of cyber safety training for school staff**

The chart shows that 50% of schools have conducted training exclusively for teaching staff, while 11% have extended it to both teaching and non-teaching staff. Additionally, 22% of schools have training planned, whereas 17% have not undertaken any training initiatives.

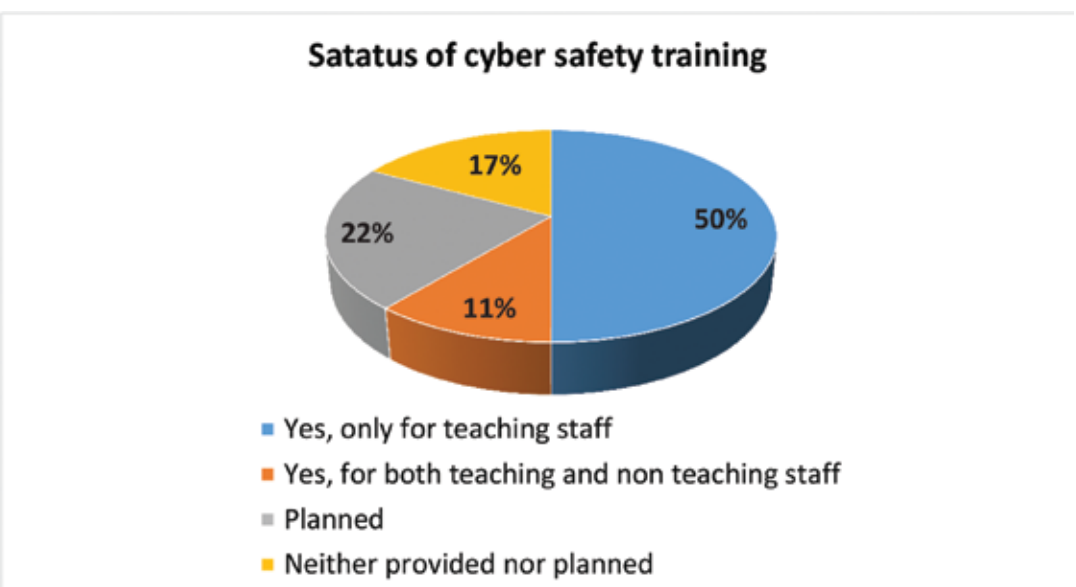



*Figure 71: Cyber safety trainings in schools*

This pattern suggests that while schools are increasingly acknowledging the importance of equipping staff with cyber safety knowledge, the majority of efforts are concentrated only on teachers. The relatively low proportion of schools including non-teaching staff points to a missed opportunity, since administrative and support staff also handle school networks, devices, and student interactions that can influence online safety. The planned initiatives show progress, but the 17% without any training highlight gaps that leave both educators and students vulnerable.

**Cyber risk reported by students at school level**

The chart on shows that a large majority of schools **(78%)** reported **no cases of cyber risks** being raised by students, while only **11% confirmed** such cases, and another **11% were not aware**.

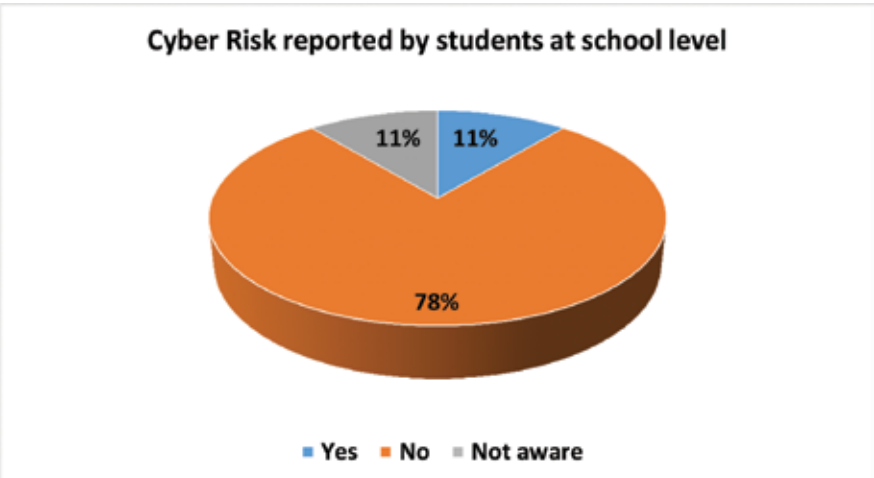



*Figure 72: Cyber risk reported by students at school level*

This finding suggests two possible interpretations. On one hand, the low reporting rate may indicate that schools have not faced major cyber incidents, or that preventive measures are effective in keeping risks under control. On the other hand, it could also point to underreporting or lack of trust in reporting mechanisms, as students might hesitate to share their experiences due to fear, stigma, or doubts about whether action will be taken. The fact that some respondents (11%) were "not aware" further highlights gaps in communication and monitoring within schools.

**Categories of online threats faced by students**

The chart highlights the diverse risks adolescents encounter in the digital space. The most significant concern identified is privacy breach (20%), reflecting growing risks around misuse of personal data, account hacking, and unauthorized sharing of sensitive information. This is closely followed by screen addiction (19%) and cyberbullying (19%), both of which directly affect students' mental health, academic focus, and overall well-being.

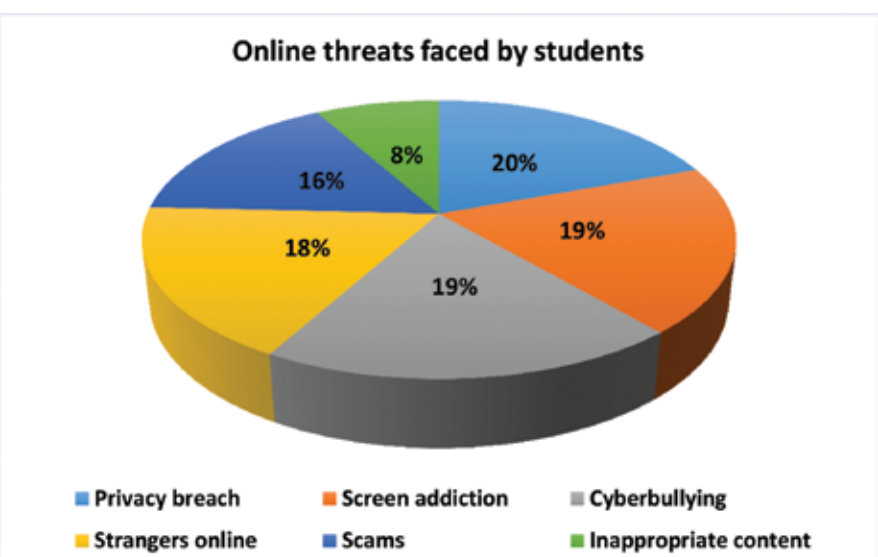



*Figure 73: Online threats reported by students*

Other prominent threats include strangers online (18%), which underscores the danger of online predators and unsafe interactions, and scams (16%), pointing to the financial and security vulnerabilities adolescents face in digital spaces. Inappropriate content (8%) is mentioned less frequently but remains a critical concern, especially given its long-term psychological impact.

From a cyber safety perspective, this highlights the need for schools to strengthen reporting and case management systems, ensure confidentiality, and build trust so that students feel safe to come forward. Moreover, training for teachers and principals in recognizing, recording, and addressing onlinesafety incidents is critical to move beyond passive acknowledgement toward proactive intervention.

**Mechanism used to report cyber risks**

The chart shows that the majority of schools (67%) rely on teachers as the primary channel for students to report online risks issues. Another 28% use anonymous complaint or suggestion boxes, while only 5% provide a dedicated email or help-desk.

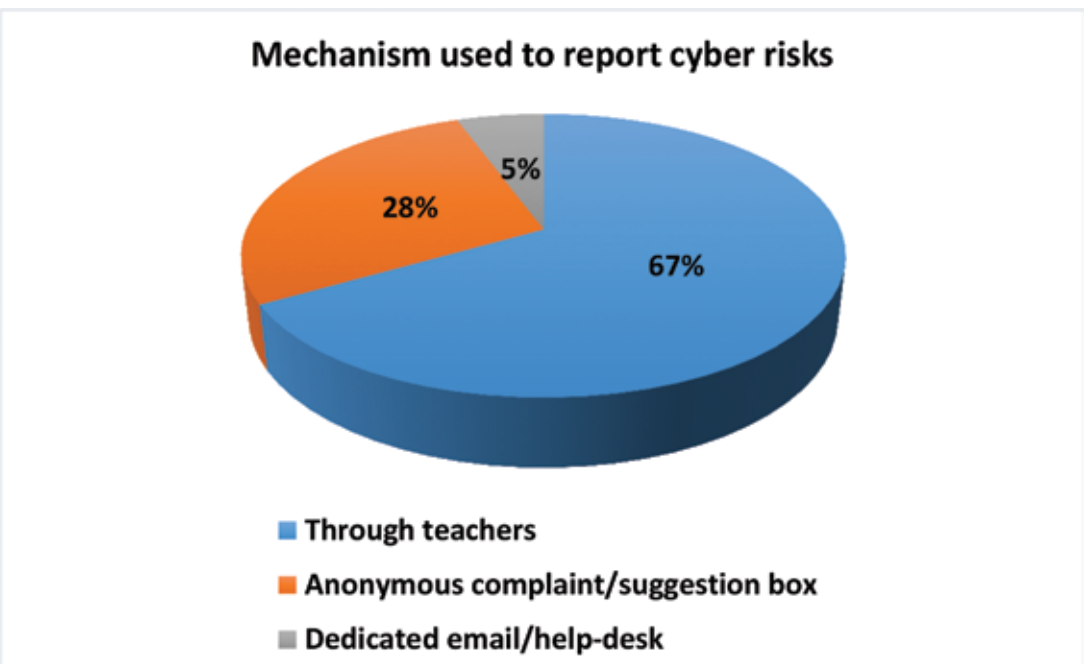



*Figure 74: Mechanisms used by students to report cyber risks*

This pattern reflects a heavy dependence on teachers, who are often the most accessible and trusted figures for students. While this approach fosters direct communication, it may also discourage reporting in sensitive cases due to fear of judgment, lack of confidentiality, or hesitation to approach authority figures. Anonymous complaint mechanisms provide more privacy, but their limited adoption shows that many schools still lack student-friendly systems. The very low use of dedicated digital reporting channels highlights a gap in integrating modern, secure mechanisms that align with today's digital environment.

Overall, the findings suggest that while schools have made efforts to establish reporting mechanisms, there is a need to diversify and strengthen these systems. Incorporating confidential digital platforms, trained counselors, and anonymous hotlines can create a safer space for adolescents to report incidents without fear, ultimately ensuring timely intervention and support.

**Challenges faced by schools to ensure cyber safety**

The chart highlights several key barriers identified by school authorities. The most significant challenge is lack of

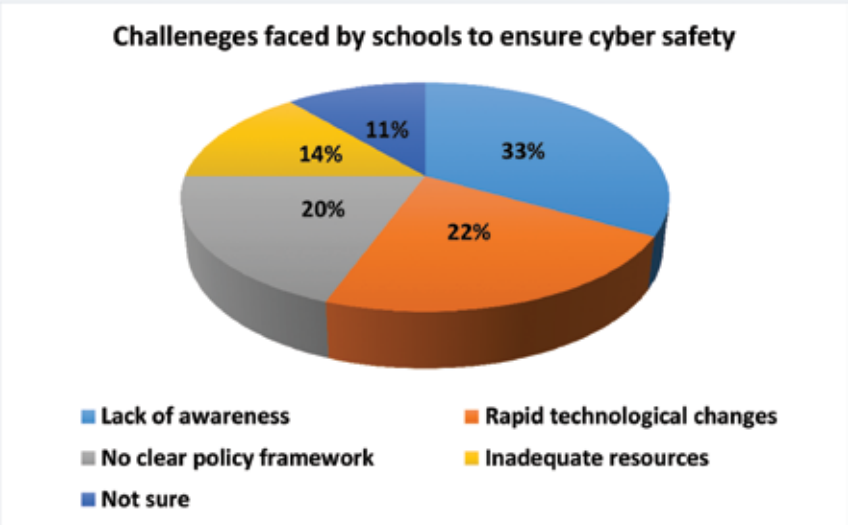



*Figure 75: Challenges faced by schools to ensure cyber safety for students*

awareness (33%), suggesting that many educators and staff may not be fully sensitized to the risks, policies, or practices needed for effective cyber safety. This is followed by rapid technological changes (22%), which make it difficult for schools to keep pace with emerging threats and evolving digital tools.

Other important issues include the absence of clear policy frameworks (20%), which creates inconsistency in how schools address online risks, and inadequate resources (14%), reflecting constraints in staff training, technical infrastructure, or financial support. A smaller proportion (11%) reported being unsure, indicating either lack of engagement with the issue or weak internal communication regarding cyber safety practices.

Overall, the findings show that while some structural and technical challenges exist, the biggest hurdle lies in awareness and preparedness. Addressing these gaps through capacity building, consistent policy enforcement, and resourceallocation will be critical for schools to create a safe digital environment for adolescents.

**Factors crucial to ensure cyber safety at school level**

The chart highlights the priority areas identified by school authorities to strengthen online safety. The most emphasized factor is implementation of government guidelines (24%), showing the importance schools place

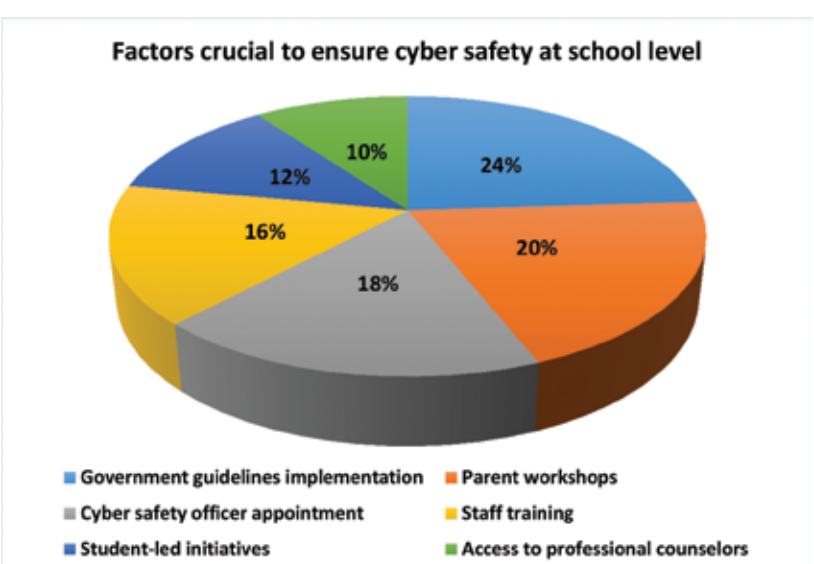



*Figure 76: Factors to ensure cyber safety in schools*

on structured policies and official directives to guide their practices. This is followed by parent workshops (20%) and cyber safety officer appointments (18%), reflecting the dual need for engaging families and establishing dedicated roles within schools to oversee safety.

Other key measures include staff training (16%), which ensures teachers are equipped with the skills to address digital risks, and student-led initiatives (12%), which recognize the role of adolescents as active agents in promoting safe online behavior among peers. A smaller share (10%) is distributed across other suggestions, underscoring that while multiple factors matter, schools tend to prioritize institutional frameworks and external guidance.

**Best practices by schools on cyber safety of adolescents**

The chart shows that 56% of schools did not share any best practices, while 17% highlighted awareness campaigns or general sensitization, another 17% emphasized cyber safety sessions or role plays, 5% mentioned individual cautious behavior, and 5% reported workshops/training for teachers and parents.


*Figure 77: Best practices in schools on cyber safety*

This finding indicates that while some schools are taking meaningful steps to promote cyber safety, more than half have either not developed structured practices or chose not to report them, reflecting a significant gap in systematic efforts. Among the practices shared, awareness campaigns and cyber safety sessions emerge as the most common strategies, showing that schools often rely on sensitization activities to build digital responsibility among students. However, relatively few examples of structured staff or parent training were reported, suggesting weaker emphasis on community-wide engagement.

**Collaboration with external agencies for cyber safety**

The chart shows that 56% of schools collaborate with external agencies such as police, NGOs, child protection units, or cyber experts, while 33% do not and 11% have plans to do so. This is a positive finding, as partnerships with external stakeholders are essential for building specialized expertise, providing timely support in case of incidents, and strengthening preventive awareness initiatives.

However, the fact that one-third of schools are not engaging with external agencies indicates a significant gap. Without such collaboration, schools may struggle to manage complex cases like cyberbullying, scams, or online harassment that require specialized intervention. The small but promising share of schools planning collaborations suggests that the practice is gradually expanding.

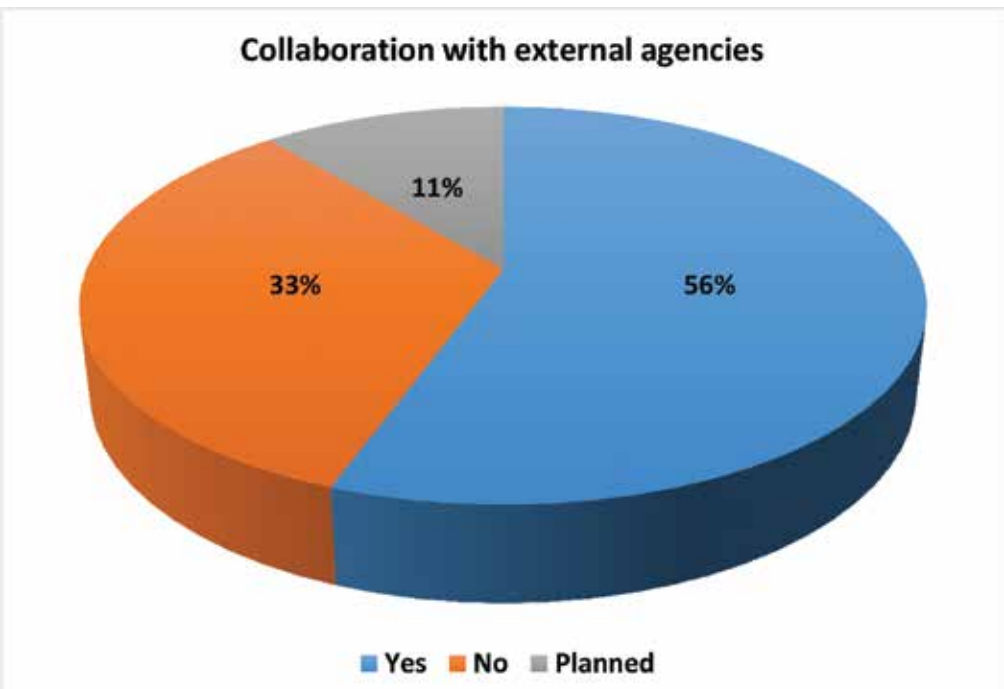



*Figure 78: Partnerships for enhancing awareness on cyber safety*

# Chapter 11: Child Welfare Committees: Oversight and Intervention in Digital Harms

**Trends in Cyber-Related Cases Involving Adolescents**

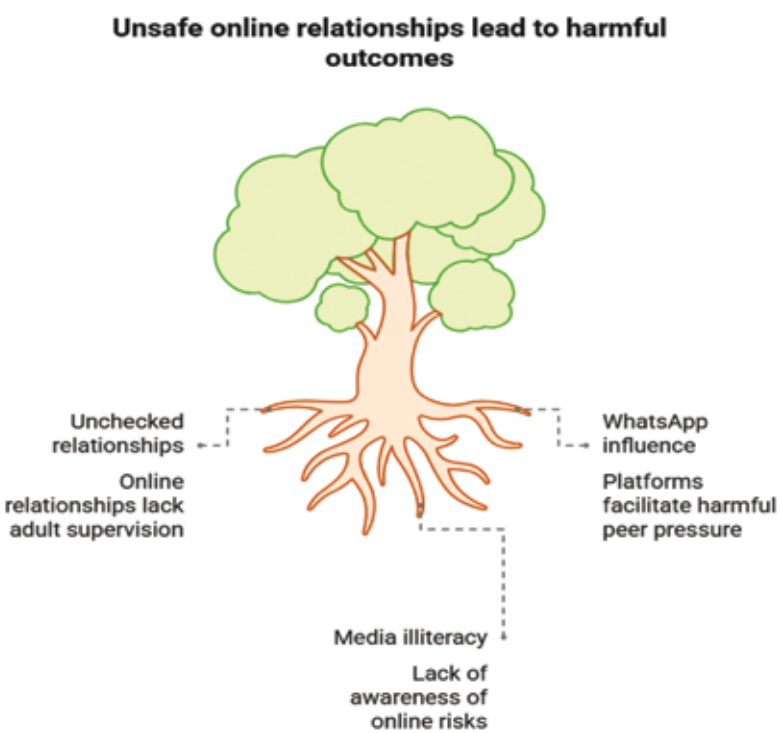
Many cases of kidnapping and missing children are linked to social media interactions. Elopement cases often originate from online relationships, where videos or photos shared during these interactions become tools for blackmail and repeated abuse.

The misuse of platforms like Instagram and Telegram is predominant among adolescent victims, as abusers use these platforms to exploit young people. Online gaming platforms and OTT content have also become sources of exposure to scams, inappropriate content, and social manipulation.

**Case story**

**"A disturbing case involved a girl who eloped after being influenced through WhatsApp chat, resulting in unwanted pregnancy and unsafe health outcomes, highlighting risks from unchecked online relationships".**

**Legal and Reporting Challenges**




Existing laws related to child protection, cybercrime, and digital privacy are fragmented. There is an urgent need for synchronizing laws under the IT and Digital Privacy Acts with those protecting children.

The Child Welfare Committee advocates for introducing a dedicated law for ***Protection of Children from Online Abuse (PCOA***) and including a distinct chapter on online digital safety and cybercrime punishments within the Juvenile Justice (JJ) Act or Delhi JJ Rules, which are currently pending.

The discussion with CWCs indicated that police agencies exhibit limited application of IT Act provisions, often

focusing only on POCSO or JJ Act cases. There is a reluctance in police to register certain cyber offences promptly, affecting timely counseling and intervention for affected children.

**Awareness and Capacity Building**

Awareness among adolescents, parents, and frontline stakeholders remains inadequate. The CWCs emphasize the need for widespread awareness campaigns through schools, parents' sensitization, and community engagement to educate about online risks and monitoring strategies.

Schools have been mandated to promote cyber safety education, including practical sessions to teach students about strong passwords, two-factor authentication, recognizing suspicious links, and safe social media practices. The Directorate of Education has integrated these measures into school assemblies and notice boards. There is a call to train police and other government stakeholders in cyber safety and child-friendly investigative approaches to ensure empathetic handling of adolescent victims.

**Technological and Social Measures**

Increasing internet accessibility among adolescents necessitates better monitoring mechanisms, including raising the age limit of unrestricted internet usage, similar to models in countries like Australia, and deploying parental controls.

Efforts to monitor darknet activity and restrict access to illegal or harmful websites need strengthening to reduce exposure to dangerous content and potential exploitation.

**Government Initiatives and Efforts**

1. The Delhi government, through the Directorate of Education and Ministry of Women and Child Development, has launched workshops, online courses, and cyber safety awareness campaigns aimed particularly at adolescents and key stakeholders.
2. CyberPeace and Delhi Police have initiated programs such as the Cyber Challenge hackathon to foster innovative cybersecurity solutions tailored to challenges like online harassment, juvenile gang activity monitoring, and digital scams.
3. National-level workshops involve multi-agency participation to improve coordination, legal understanding, and implement best practices in cyber threat mitigation.

**Underreporting and Registration Barriers**

Officers noted that the recorded number of complaints is substantially lower than actual incidents experienced by cybercrime victims. Procedural difficulties, lack of awareness about reporting mechanisms, and a tendency among victims—particularly adolescents—to avoid formal complaints contribute to underreporting.

**High-Tech Cybercrime Networks**

Recent investigations by Delhi Police's Intelligence Fusion and Strategic Operations (IFSO) unit have exposed large scale cybercrime syndicates exploiting technological loopholes. In one case, police recovered over 6.5 kg of SIM cards during a probe linked to the cybercrime hub of Jamtara, Jharkhand, indicating the scale and operational complexity of phone-related cyber fraud.

**Clear Complaint Channels and User Support**

The police delineate complaint registration wherein economic offence complaints go through helpline '1930', while non-economic cybercrime cases are directed to cybercrime@gov.in. However, the practical accessibility of these channels remains a concern, as many users find portals difficult and helplines busy. Use of WhatsApp or SMS for complaint registration is coined as a more user-friendly alternative by police officers.

**Device Usage Patterns among Adolescents**

Most children access the internet via family-owned devices such as mobiles, laptops, and tablets. Approximately 90% of adolescent victims use Android devices, with the remaining 10% on iOS. This device distribution aligns with economic demographics and Android's widespread availability at affordable prices.

**Financial Impact and Banking Responses**

When cyber fraud is reported, banks routinely freeze compromised accounts at police request, helping curb losses. Youth engaged in online gaming often also involve bank transactions, increasing risk exposure. Detection of suspicious transactions initiates immediate frozen status to prevent further fraud.

# Chapter 13: Recommendations& Conclusion

**Policy-Oriented Recommendations**

It is necessary to adopt a number of legislative and policy actions to fortify the legal frameworks pertaining to the safety of adolescents online. The goal of these suggestions is to give young people a safer and more secure online environment while maintaining the harmony between privacy, protection, and freedom of speech.

**A. Embedding Cyber-laws in education system**

**Integration into Education Policy& Curriculum:** Evidence shows adolescents lack strong cyber safety practices (e.g., 45% never change passwords, 41% accept friend requests from strangers). This necessitates embedding cyber safety education modules into the National Education Policy (NEP) framework in partnership with NCERT & SCERTs.

**School ComplianceMechanism:** The uneven adoption of cyber safety policies (83% exist but only 61% implemented) indicates the need for mandatory school-level compliance mechanisms, monitored through Directorate of Education in Delhi and in other states as well.

**Strict implementation of Guidelines on Child Safety & Security:**The National Commission for Protection of Child Rights (NCPCR) has issued guidelines on Child Safety and Security that, although often framed around schools, institutions, and child rights broadly, have direct implications for online digital safety of adolescents.The guidelines emphasize creating safe, non-threatening environments where children can learn and thrive.This means mandating age-appropriate digital platforms, stronger privacy defaults, and restricted access to harmful sites on school devices.

**B. Strengthening Child-Centric Cyber Laws in India**

**Explicit Law on Juvenile Online Safety:**

That address all aspects of juvenile online safety, including data privacy, cyberbullying, online exploitation, and digital addiction.Delivering on these reforms will require coordinated action across multiple stakeholders. The Ministry of Electronics and Information Technology (MeitY) can take the lead in drafting the Child Online Safety Law and enforcing compliance, while the Ministry of Women and Child Development (MWCD) and the National Commissions on Child Rights and Human Rights may oversee awareness campaigns and monitoring.

**New Child Online Safety Authority:**

Establishment of an independent regulator under the new law on Juvenile Online Safety to enforce adolescent online safety norms.It could be modelled itself on the UK's Ofcom under Online Safety Act or Ireland's Data Protection Commission.A New Child Online Safety Authority (COSA) in India could play a pivotal role in filling current policy and regulatory gaps around adolescent digital safety. Right now, responsibilities are fragmented: MeitY (IT Rules, intermediaries), MWCD (POCSO, child rights), and NCPCR (guidelines and monitoring). A specialized authority would consolidate oversight, enforcement, and coordination—similar to how child protection regulators in other countries have evolved.

*Table 2: Child Online Safety Authority*

| Child Online Safety Authority Comparative Snapshot | | | | |
|---|---|---|---|---|
| **Feature** | **UK (Ofcom)** | **Australia (eSafety)** | **EU (DSA/GDPR)** | **Proposed COSA (India)** |
| **Dedicated child regulator?** | Ofcom (expanded role under Online Safety Act) | Yes — eSafety Commissioner | No single child regulator (DSA + national authorities) | Yes — COSA (statutory) |
| **Mandatory risk assessments?** | Yes | Yes | Systemic risk obligations for large platforms | Yes — Child Impact Assessments mandated |
| **Rapid takedown SLAs?** | Enforced obligations | Rapid takedown for image abuse | Varies | 24–48 hr target for CSAM/deepfakes |
| **Algorithm audits?** | Powers to audit | Remedial powers & engagement | Required for large platforms | Independent audit authority within COSA |
| **Single-window complaints?** | No single child portal (platforms + Ofcom) | Yes — eSafety portal | Varies by member state | Yes — integrated portal linked to 1098 |
| **Privacy safeguards for age checks?** | Required | Required | GDPR constraints | Privacy-preserving age assurance mandated |

**C. Platform-centric regulatory model**

Adolescents are among the fastest-growing internet user groups in India, but they lack bargaining power to influence platform policies. Current laws (like IT Act, IT Rules 2021, and POCSO) either:

- Focus on criminal liability after harm (e.g., child sexual abuse material), or
- Place the burden on parents/educators to supervise use.

This creates a protection gap because platforms, which design addictive features, track user data, and allow harmful content to circulate, escape direct obligations. A platform-centric model fixes this imbalance by embedding safety into design and governance of digital ecosystems. Some of the key-features of platform-centric regulatory framework are:

**1. Age-Appropriate Design Code**

a. Platforms must design services suitable for under-18 users, with stricter protections for under-13s and 13–16 group.

b. Default privacy settings should be “high” for minors (e.g., no geo-location sharing, limited contact options).

c. Ban/restrict features like autoplay, targeted ads, infinite scroll, or loot boxes that exploit adolescent vulnerabilities.

**2. Risk-Based Due Diligence**

Platforms should conduct child safety risk assessments before launching features (similar to Environmental Impact Assessments). This includes evaluating risks of grooming, bullying, addictive usage, or exposure to harmful content. Regulatory authority (like MeitY, NCPCR, NHRC etc.) could review these assessments.

3. **Transparency & Accountability Mechanisms**

Platforms must publish quarterly transparency reports on content takedowns, cyberbullying complaints, and harmful content flagged by Indian users. Independent audits of algorithmic systems to check if they amplify harmful or unsafe content for adolescents.

4. **Age Verification & Assurance**

It should be mandatory to have privacy-preserving age verification mechanisms to restrict minors from accessing harmful services (e.g., pornographic sites, betting apps).Encourage use of digital guardianship tools with clear opt-ins for parents/adolescents.

5. **Programmatic and Operational Recommendations**

1. **School-Level Interventions:**

- Institutionalize regular cyber safety sessions in schools with clear monitoring indicators.
- Create adolescent-led groups ("Cyber Yodhas") as peer educators.
- Establish confidential complaint mechanisms (digital portals, helplines, counselors) accessible to students.

2. **Parental Engagement Interventions:**

- Develop structured parental workshops on digital parenting, with modules tailored for parents.
- Promotion of community-based awareness campaigns in local languages to build digital literacy among parents.

3. **Institutional Strengthening Interventions:**

- Support CWCs and police in creating child-friendly reporting systems and fast-tracking cybercrime cases involving minors.
- Facilitate joint training programs for school staff, police, and NGOs to standardize responses to cyber incidents.

4. **Community-Level Interventions:**

- Launch mass digital literacy campaigns with culturally resonant messaging through radio, social media, and community platforms.
- Establish adolescent cyber clubs at community centers to foster safe digital learning environments.

**Conclusion**

Child online safety cannot be treated as an afterthought to India's digital revolution. Without urgent intervention, the risks posed by unregulated platforms and emerging technologies will disproportionately harm adolescents, who form the most active segment of India's digital users. A Unified Child Online Safety Law, coupled with platform accountability, institutional capacity, and future-proof laws, represents the most sustainable pathway forward.

Investing in child online safety is not optional—it is the foundation of India's digital future.Government, donors, civil society partners and individuals can play a catalytic role by supporting evidence-driven advocacy, capacity building, and amplifying children's voices in policymaking. With coordinated action, India can not only protect its young digital citizens but also set a global benchmark for child-centric cyber governance.

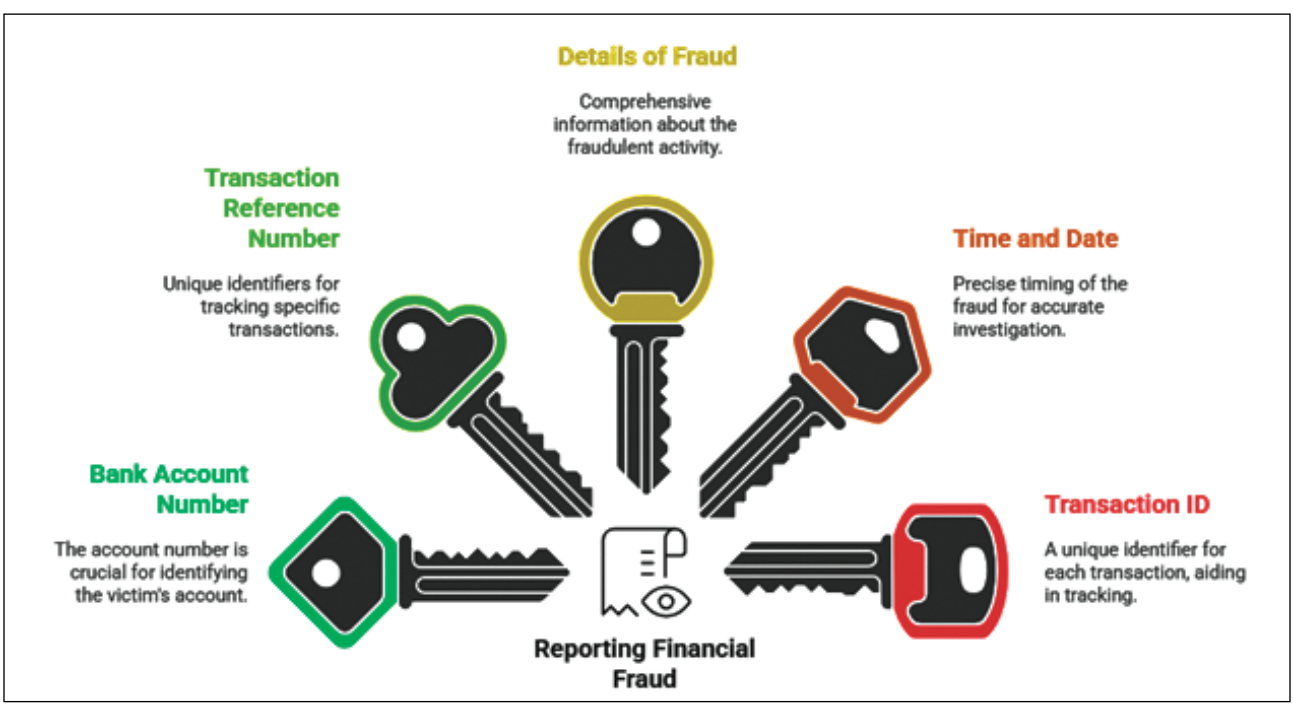
# About Cyber Crime Unit – Delhi Police

The Intelligence Fusion & Strategic Operations, IFSO of Delhi Police functions under the Special Cell and is a specialized unit that handles all complex and sensitive cases of cybercrime including those in which victims are women and children[1].

**In case of cyber financial fraud, note these five things and then dial 1930.**

1. Bank Account Number
2. Unique Transaction Reference Number (16 digits for NEFT, 22 digits for RTGS & 12 digits for UPI]
3. Complete detail of financial fraud
4. Correct time and date of financial fraud
5. Transaction ID

[1]https://cyber.delhipolice.gov.in/



# List of District Wise Cyber Police Station

| 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 | | | |

# References
# (APA 7th Edition)


Akter, M., Park, J. K., & Wisniewski, P. (2025). *Moving beyond parental control toward community-based approaches to adolescent online safety* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2501.01234

Directorate of Education, Delhi. (2025, May 25). Delhi schools promote digital safety awareness to prevent cybercrimes among students and staff. *The Times of India.* https://timesofindia.indiatimes.com

Immersive Metaverse Study. (2025). Immersive metaverse learning for children's cyber harm prevention. *Journal of Educational Technology Research, 18*(2), 45–62. https://doi.org/10.xxxx/metaverse2025

Jang, Y. (2023). Online safety for children and youth under the 4Cs risk framework. *Frontiers in Psychiatry, 14,* 1053252. https://doi.org/10.3389/fpsyt.2023.1053252

Kaiser, S. (2021). An app-based intervention for adolescents exposed to cyberbullying or negative online experiences in Norway: Development and pilot testing of NettOpp. *JMIR Research Protocols, 10*(11), e31789. https://doi.org/10.2196/31789

Lahti, H., Kiviruusu, O., &Marttunen, M. (2024). Social media threats and health among adolescents. *Child and Adolescent Psychiatry and Mental Health, 18,* 754. https://doi.org/10.1186/s13034-024-00754-9

Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics, 5,* 143–158. https://doi.org/10.2147/AHMT.S36456

Park, J., Akter, M., Ali, N. S., Agha, Z., Alsoubai, A., & Wisniewski, P. (2025). *Towards resilience and autonomy-based approaches for adolescents online safety* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2501.04567

Schulz, P. J., Bullo, P., & Sibilio, M. (2025). Adolescent cyberbullying and cyber victimization: A longitudinal study. *Journal of Medical Internet Research, 27,* e70508. https://doi.org/10.2196/70508

World Economic Forum. (2025, January 18). Tackling digital safety challenges to create a safer world. *World Economic Forum.* https://www.weforum.org

Zhu, X. (2024). Surfing into trouble? How internet use influences early adolescent externalizing problem behaviors. *Humanities and Social Sciences Communications, 11,* 222. https://doi.org/10.1057/s41599-024-02722-2

Australian eSafety Commissioner. (n.d.). *Safety by Design: Principles and guidance*. https://www.esafety.gov.au/industry/safety-by-designeSafety Commissioner

Department for Science, Innovation and Technology (DSIT). (2025). *Online Safety Act collection & explainer*. GOV.UK. https://www.gov.uk/government/collections/online-safety-actGOV.UK+1

Digital Wellness Lab. (2024). *The online experiences of LGBTQ+ youth*. https://digitalwellnesslab.org/research-briefs/the-online-experiences-of-lgbtq-youth/The Digital Wellness Lab

Eyal, K., Benalka, Y., & Vidas, M. (2024). Characteristics and outcomes of interventions for teaching digital media literacy: A systematic review. *Journal of Children and Media, 18*(4), 523–545. https://doi.org/10.1080/17482798.2023.2265510

Global Kids Online—India. (2022). *Country report (Final)*. https://globalkidsonline.net/india/ (PDF link in page). globalkidsonline.net+1

Information Commissioner's Office (ICO). (2021–2025). *Age-Appropriate Design Code (Children's Code)*. https://ico.org.uk/…/age-appropriate-design-a-code-of-practice-for-online-services/

Jeong, S.-H., Cho, H., & Hwang, Y. (2012). Media literacy interventions: A meta-analytic review. *Journal of Communication, 62*(3), 454–472. https://doi.org/10.1111/j.1460-2466.2012.01643.x

Jang, Y. (2023). Online safety for children and youth under the 4Cs risk framework. *Frontiers in Psychiatry, 14*, 1053252. https://doi.org/10.3389/fpsyt.2023.1053252

Kamaruddin, I. K., Rahman, N. A. A., & Bahar, N. (2023). Interventions to prevent school-based cyberbullying: A systematic review and meta-analysis. *BMC Public Health, 23*, 118. https://doi.org/10.1186/s12889-022-14678-5

Kutok, E. R., et al. (2021). A media-based intervention to prevent adolescent cyber-conflict: A pilot randomized trial. *JMIR Mental Health, 8*(9), e26029. https://doi.org/10.2196/26029

McAlister, K. L., et al. (2024). Social media use in adolescents: Bans, benefits, and emotion regulation. *JMIR Mental Health, 11*, e64626. https://doi.org/10.2196/64626

OECD. (2024). *Towards digital safety-by-design for children*. https://doi.org/10.1787/f1c86498-en

Polanin, J. R., Espelage, D. L., &Grotpeter, J. K. (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying. *Prevention Science, 23*, 439–454. https://doi.org/10.1007/s11121-021-01259-y

Qamaria, R. S., et al. (2025). Digital resilience in adolescence: A systematic review. *Malaysian Management Journal, 29*(1), 1–17. (Open-access PDF).

Rachmayanti, R. D., et al. (2024). Using digital media to improve adolescent resilience and well-being: Systematic review protocol. *JMIR Research Protocols, 13*, e58681. https://doi.org/10.2196/58681

Ren, W., et al. (2022). Parental mediation and adolescents' internet use: A meta-analysis. *International Journal of Environmental Research and Public Health, 19*(6), 3424. https://doi.org/10.3390/ijerph19063424

Stoilova, M., Livingstone, S., &Khazbak, R. (2021). *Investigating risks and opportunities for children in a digital world: A rapid review*. UNICEF-Innocenti. https://www.unicef.org/innocenti/publications UNICEF

Gupta, A., & Singh, P. (2019). The psychological impact of cyberbullying on Indian adolescents: A comparative study. *Journal of Youth Studies in Asia, 7*(2), 112-128.

Jain, S. (2020). *Digital inclusion and risk: A report on internet penetration and user behavior in urban India*. NITI Aayog Press.

Ministry of Home Affairs. (2022). *Cybercrime prevention against women and children (CCPWC) scheme*. Government of India.

National Commission for Protection of Child Rights (NCPCR). (2021). *Report on the prevalence of online child sexual abuse material in India*. Government of India.

Pal, R., & Sen, B. (2018). Online harassment and trolling as a tool for silencing women in India. *Gender & Digital Society, 4*(1), 22-35.

Sharma, R., & Mishra, A. (2018). Challenges in prosecuting cybercrime in India: A legal analysis. *Journal of Indian Legal Studies, 12*(3), 45-60.

Tiwari, V. (2021). *The new battlefield: Cyberstalking and doxing against women in contemporary India*. Cybercrime and Justice in the Global South, 15(4), 210-225.


**Regd. Address:** O-35, Sri Niwas Puri, Delhi - 110065

**Project Office:** Matri Sudha Children Resource Centre, Basti Vikas Kendra, Nardan Basti, M B Road, Lal Kuan, Delhi - 110044

**Contact:** 96-25-96-3443

https://matrisudha.org/