International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

# HOW TO PROTECT CHILD ONLINE

*Muskan Yadav*[1]*,Avinash Mishra*[2]

(22GSOB1010756)
[2] Under the supervision of
Galgotias University

## INTRODUCTION

In the digital age, children are increasingly exposed to online environments for education, entertainment, and communication. While the internet offers vast opportunities, it also poses significant risks, including cyberbullying, online predators, inappropriate content, and privacy violations. This report explores the growing need to protect children online, examining the current threats, parental and institutional responsibilities, and technological safeguards.

The internet has become an indispensable part of modern life, offering children vast resources for learning, creativity, and social interaction. From online classes to gaming and social media, children today are more digitally connected than ever before. However, this increased connectivity also exposes them to numerous online threats such as cyberbullying, grooming by predators, exposure to inappropriate content, identity theft, and privacy breaches.

As digital natives, children may lack the maturity and awareness needed to recognize and handle these risks. Many are unaware of how to respond to online harassment or report unsafe behavior. At the same time, parents and educators often struggle to keep up with rapidly evolving technologies and digital platforms. The responsibility to protect children online, therefore, must be shared among families, schools, tech companies, and policymakers.

This report aims to investigate the challenges of online safety for children, identify existing protective measures, and recommend practical strategies to create a safer online environment for young users. It highlights the urgent need for a proactive approach that combines education, awareness, and technological safeguards.

In the digital age, the internet has become an integral part of children's daily lives, providing vast opportunities for learning, social interaction, creativity, and entertainment. With online education platforms, games, video-sharing services, and social media, children are more connected than ever before. However, this increased connectivity comes with serious safety concerns.

Children face a multitude of online risks including cyberbullying, exposure to inappropriate content, online predators, identity theft, and privacy violations. They may unknowingly engage in unsafe behavior, such as sharing personal information, clicking on malicious links, or interacting with strangers. These threats are compounded by the rapid evolution of digital technology and the complexity of online platforms, which often outpace protective regulations and parental oversight.

Moreover, children are often unaware of the long-term implications of their online actions, making them more vulnerable to exploitation. This vulnerability is further intensified by a lack of adequate digital literacy and guidance from adults. In many cases, parents and educators themselves struggle to keep up with the fast-changing digital landscape.

This report delves into the growing need to protect children online. It examines prevalent online threats, evaluates the roles of parents, educators, governments, and technology providers, and assesses the effectiveness of current safety measures. The goal is to recommend actionable strategies and promote a safer, more empowering digital environment for children everywhere.

### *OBJECTIVE OF THE STUDY*

The growing prevalence of internet access among children has introduced a wide range of opportunities for learning and communication, but it has also exposed them to significant risks such as cyberbullying, online predators, privacy violations, exposure to inappropriate content, and digital addiction. The aim of this study is to understand how young adults—particularly undergraduate students in Delhi NCR—perceive and respond to these risks. The research seeks to identify knowledge levels, behavior patterns, and attitudes that can influence the development of safer online environments for children. The detailed objectives of the study are outlined below:

**1. To Assess Awareness of Online Risks Faced by Children**

- Exposure to explicit or harmful content
- Online grooming and exploitation
- Cyberbullying and peer harassment

**2. To Examine the Use of Parental Control Tools and Supervision Practices**

- Parental control apps

- Monitoring software
- Screen time and content restrictions

**3. To Determine Perceptions of the Appropriate Age for Device Ownership**

- What age is considered developmentally suitable for owning a smartphone or tablet
- Whether early exposure is seen as risky or beneficial

**4. To Evaluate the Frequency and Quality of Communication about Online Safety**

- How often respondents believe children should be guided about internet safety
- Whether discussions about privacy, cyberbullying, and digital etiquette are encouraged
- The perceived importance of parental or adult involvement in open digital communication
  This reflects how much emphasis is placed on preventive education within homes and communities.

**5. To Identify Perceived Responsibility for Child Online Safety**

- Parents and guardians
- Schools and teachers
- Government and regulatory bodies
- Technology companies

**6. To Understand Perceptions of School Programs on Digital Safety**

- Whether schools are currently seen as effective in teaching digital citizenship and safety
- The presence or absence of formal programs related to online behavior

**7. To Analyze Attitudes Toward Child-Safe Features in Apps and Websites**

- Age-appropriate content
- Strong privacy settings
- Reporting/blocking tools
- Absence of ads and in-app purchases

**8. To Identify Platforms Perceived as Most Risky for Children**

- Which platforms are viewed as unsafe (e.g., Instagram, YouTube, Snapchat, etc.)
- What features or functions make them risky
- How respondents believe these platforms could be improved
  These insights can inform digital platform developers and regulators on where and how to tighten safety measures.

**9. To Gather Recommendations for Improving Child Online Safety**

- Policy improvements
- Parental or community actions
- Educational interventions
- Technological innovations
  These recommendations are vital in building a collaborative, realistic, and youth-informed framework for protecting children online.

## *SCOPE OF THE STUDY*

This study focuses on understanding the various dimensions of online safety for children aged 6 to 17 who regularly access the internet for education, entertainment, social interaction, and communication. It covers a broad spectrum of digital platforms and services that children typically engage with, including:

The present study, titled *"How to Protect Children Online,"* aims to explore the awareness, perceptions, and proposed solutions related to online child safety among undergraduate students in the Delhi NCR region. The study is framed within a digital context that is increasingly influencing children's lives, education, entertainment, and social interactions. Given the growing exposure of children to online platforms, understanding how young adults—who are future parents, educators, and professionals—perceive and approach child protection in the digital space is both relevant and necessary.

**1. Thematic Scope**

The study focuses on the following key thematic areas:

- **Awareness of Online Risks**: Evaluating the respondents' understanding of risks such as cyberbullying, exposure to inappropriate content, online predators, privacy violations, and digital addiction.
- **Parental Control and Technology Use**: Examining the usage and perceptions of digital monitoring tools like parental control apps, screen-time management, and content filters.
- **Communication and Guidance**: Investigating how often young adults believe children should be spoken to about online safety and the importance of such communication.

- **Opinions on Responsibility**: Identifying whom respondents believe should be responsible for ensuring child safety online—parents, schools, governments, tech companies, or children themselves.
- **Risky Platforms and Content**: Understanding perceptions of which digital platforms are most harmful to children and what features are considered essential for making apps and websites child-safe.
- **Age-Appropriateness and Device Ownership**: Analyzing opinions on the appropriate age for children to own smartphones or personal devices.

**2. Demographic Scope**

- **Geographic Focus**: The study is limited to Delhi NCR, a metropolitan region in India known for high internet penetration, educational access, and exposure to digital technology. This urban focus provides insight into digitally literate youth, but does not cover rural or less-developed areas where digital awareness and access may differ significantly.
- **Respondent Profile**: The study targets undergraduate students, aged approximately between 18 and 24 years. Though they may not yet be parents, their perspectives are valuable for understanding emerging generational attitudes toward digital responsibility, child safety, and technology use.

**3. Methodological Scope**

- The study is based on primary data collected through structured questionnaires using descriptive statistical analysis to interpret the responses.
- It includes quantitative data only, limiting the exploration of deeper qualitative experiences or narratives related to parenting, trauma, or digital intervention.
- The research uses convenience sampling, which restricts randomness but allows for efficient data collection within available resources and time constraints.

**4. Temporal Scope**

- The research was conducted during a specific time period (e.g., May–June 2025) and reflects attitudes and knowledge at that moment.
- It does not account for evolving perceptions over time or the impact of new technological developments, policies, or media events related to online safety.

**5. Institutional and Technological Scope**

- The study includes respondents' views on the role of schools, government agencies, and technology companies in online child protection.
- It covers popular social media and messaging platforms such as Instagram, WhatsApp, YouTube, Facebook, and Snapchat, which are widely used by children and youth in India.

**6. Limitations within the Scope**

- **Excludes actual parents and children**: The study does not directly involve parents or children—key stakeholders in digital safety—which limits the practical applicability of the findings.
- **Excludes rural and semi-urban perspectives**, which may show different levels of digital literacy, access, and parental supervision.
- **Excludes qualitative insights**, such as personal experiences, emotional responses, and real-life incidents, which would enrich the understanding of digital threats and protection strategies.

## LITERATURE REVIEW

The proliferation of digital technologies has fundamentally altered childhood experiences. While the internet offers vast educational and social opportunities, it also exposes children to significant risks. As such, scholars, policymakers, and child advocacy organizations have examined various protective strategies. This literature review explores current research on child online protection, focusing on regulatory frameworks, technological solutions, digital literacy, parental involvement, educational interventions, and multi-stakeholder approaches.

The exponential growth of digital technology has transformed the way children interact with the world, offering both opportunities and significant risks. The literature on child online safety spans multiple domains, including digital literacy, parental supervision, policy intervention, and platform accountability. This review synthesizes existing academic research, government reports, and international guidelines to contextualize the findings of the present study, which explores how young adults perceive and engage with issues related to online child protection.

**1. Awareness and Understanding of Online Risks**

Multiple studies underscore that awareness of online risks is the first step in preventing harm. According to Livingstone and Helsper (2007), awareness among youth about digital threats is shaped by education, media exposure, and parental influence. UNICEF (2021) emphasizes that while many individuals are aware of common risks such as cyberbullying and privacy violations, deeper understanding—such as how algorithms influence content exposure or how data is collected—is often lacking. This aligns with the current study's finding that although 80% of respondents are familiar with online risks, 20% still lack comprehensive understanding, highlighting the need for targeted awareness programs.

**2. Parental Supervision and Digital Parenting**

Research consistently shows that parental involvement plays a critical role in ensuring online safety. According to the Cyberbullying Research Center (Patchin & Hinduja, 2018), the use of parental control software and regular communication between parents and children significantly reduces the likelihood of cyber threats. Kapoor and Sharma (2022) note that in India, digital parenting is still emerging, with many parents lacking the skills or tools needed to monitor children's online behavior. In the current study, while 58% of respondents reported using parental control tools, a substantial proportion still lacked consistent communication with children—indicating a gap between tool usage and active parental engagement.

**3. Age of Digital Independence**

There is growing international consensus that the timing of children's exposure to personal devices should be guided by both age and maturity. The American Academy of Pediatrics (AAP) recommends delaying smartphone ownership until at least age 13, while encouraging supervised digital engagement beforehand. The findings of the present study, in which 76% of respondents support smartphone ownership at age 15 or older, resonate with this view and highlight a cautious approach that prioritizes developmental readiness over convenience.

**4. Role of Schools in Online Safety Education**

Schools are recognized as key stakeholders in digital education. ITU (2020) and Ofcom (2023) both recommend the integration of digital literacy into national education systems. However, existing research shows a lack of uniformity in implementation. According to the National Crime Records Bureau (NCRB, 2023), many Indian schools have limited resources to address online safety comprehensively. In this study, respondents had mixed perceptions of school program effectiveness, with 32% stating programs are ineffective and 10% unaware of their existence, confirming prior research findings that school efforts need more consistency and visibility.

**5. Platform-Specific Risks**

Social media platforms have been widely studied for their role in exposing children to online harm. Instagram, for example, has been criticized for its impact on mental health and exposure to sexual content (UNICEF, 2021; Common Sense Media, 2022). Platforms like Snapchat and WhatsApp, with features like disappearing messages and end-to-end encryption, pose unique monitoring challenges. In the current study, Instagram was perceived as the riskiest platform (50%), followed by Snapchat, Facebook, and WhatsApp—aligning with global trends that highlight these platforms as primary sources of risk for minors.

**6. Shared Responsibility and Stakeholder Roles**

The literature emphasizes that child online protection is a shared responsibility among parents, schools, governments, technology companies, and children themselves. The ITU (2020) advocates for a “multi-stakeholder framework” that promotes collaboration across sectors. The study supports this model, showing that while 43% of respondents see parents as primarily responsible, others recognize the importance of schools, regulators, and tech companies. This reflects a broader understanding of the need for systemic change, not just household-level supervision.

**7. Essential Features of Child-Friendly Platforms**

Several studies have explored the design features that make digital platforms safer for children. According to Google Safety Center and UNICEF guidelines, age-appropriate content, strong privacy settings, ad-free environments, and easy reporting mechanisms are essential. The current study’s findings align with this, as most respondents prioritized these features, particularly age-appropriate content and parental supervision tools.

***Summary of Literature Gaps and Relevance***

While the existing literature offers strong support for the findings of this study, it also points to several gaps—particularly in terms of implementation in the Indian context, digital parenting capacity, and consistent school programs. This study contributes to the literature by offering a youth perspective—often overlooked—on how child safety can be practically achieved and who should be responsible. It also emphasizes the need for better coordination between education, technology, and policy to create a comprehensive child online protection ecosystem.

## RESEARCH METHODOLOGY

The methodology for this study is designed to comprehensively explore the various risks and protective measures associated with children’s online experiences. Given the sensitive and multidimensional nature of the topic, a mixed-methods approach was adopted, combining both quantitative and qualitative techniques to gain depth, accuracy, and holistic insights.

This section outlines the systematic approach adopted to conduct the research study titled *"How to Protect Children Online"*. It includes the research design, objectives, sampling method, data collection tools, analysis techniques, and ethical considerations. The methodology was structured to ensure that the data collected would be both relevant and reliable for examining awareness levels, attitudes, and practices related to online child safety among youth.

1. **Research Design**

The study followed a descriptive research design, which is suitable for understanding current trends, opinions, and behaviors related to a particular issue—in this case, online child protection. This design allowed for the collection and interpretation of data from a defined population to gain insights into their knowledge, perceptions, and suggestions regarding children’s online safety.

2. **Research Objectives**

The key objectives of the research were:

- To assess the level of awareness among youth regarding the risks children face online.
- To identify the common practices used for supervising children's internet activities.
- To understand perceptions about the appropriate age for digital independence.
- To evaluate opinions on who holds responsibility for child online safety.
- To gather suggestions on how digital platforms and institutions can enhance child protection.

3. **Population and Sample**

The target population for this study comprised undergraduate students in the Delhi NCR region, as they represent a group of digitally literate young adults who may become future parents, educators, or policymakers.

- Sampling Method: The study used a non-probability convenience sampling technique due to accessibility and time constraints. This allowed the researcher to gather data from willing participants who were easily available.
- Sample Size: A total of 60 respondents participated in the study. While this number is not large enough to generalize results across all demographics, it provides useful insights for exploratory research.

4. **Data Collection Method**

The study employed primary data collection through a structured questionnaire designed specifically for this research. The questionnaire was divided into thematic sections:

- Awareness and understanding of online risks
- Use of technology and parental controls
- Opinions on digital behavior and device usage
- Views on institutional roles (schools, government, tech companies)
- Recommendations for online child safety

The questions were mostly close-ended, including multiple-choice, Likert scale, and categorical response options to facilitate statistical analysis.

- Mode of Data Collection: The questionnaire was administered through Google Forms, allowing participants to respond digitally and anonymously.

5**. Tools of Analysis**

The data collected was analyzed using descriptive statistical tools, primarily:

- Frequency distribution
- Percentages
- Tabulation
- Graphical representation (e.g., bar charts, pie charts where applicable)

These tools helped interpret the data in a clear and accessible way, making it easier to draw conclusions in alignment with the study objectives.

6. **Scope of the Study**

The scope of the study is limited to understanding youth perspectives—specifically those of undergraduate students—on protecting children online. While it does not include responses from actual parents or children, it sheds light on future parenting attitudes, digital awareness, and the expectations of younger generations regarding institutional roles in online safety.

7. **Ethical Considerations**

The following ethical practices were observed:

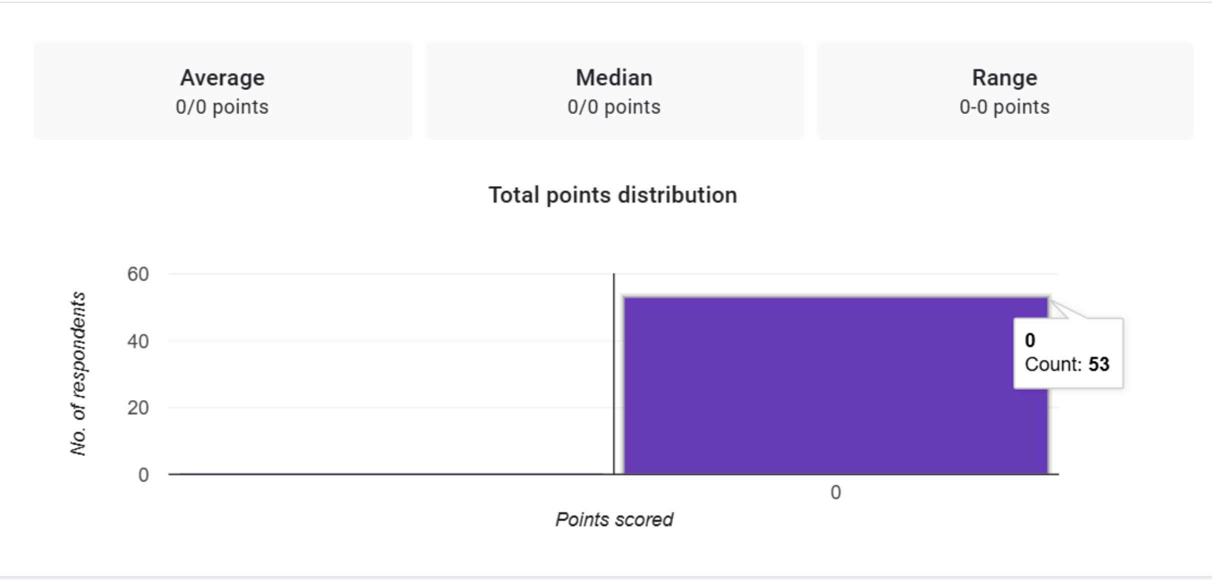
- Informed Consent: All participants were informed about the purpose of the study before submitting their responses.

- Anonymity and Confidentiality: No personal identification data was collected. All responses were kept anonymous and used strictly for academic purposes.

- Voluntary Participation: Participation was entirely voluntary, with no pressure or incentive involved.

8. **Limitations of the Methodology**

While the methodology ensured structured and focused data collection, the use of a convenience sample, limited geographic coverage, and lack of qualitative input from parents or children are acknowledged limitations. These restrict the generalizability of the findings and indicate the need for broader future studies.



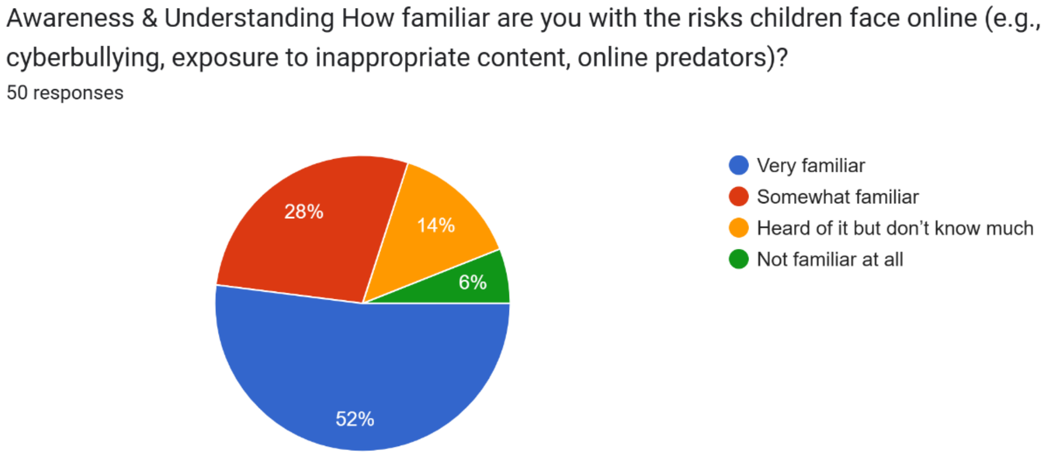
Average
0/0 points

Median
0/0 points

Range
0-0 points

## DATA ANALYSIS AND INTERPRETATION

This chapter presents the analysis of primary data gathered from 60 undergraduate students in Delhi NCR. The aim is to uncover trends, knowledge gaps, and attitudes related to online child safety. The data, obtained through structured questionnaires, is interpreted using descriptive statistics—percentages, means, and graphical representations—to draw insights aligned with the research objectives●



Awareness & Understanding How familiar are you with the risks children face online (e.g., cyberbullying, exposure to inappropriate content, online predators)?
50 responses

**Awareness & Understanding**

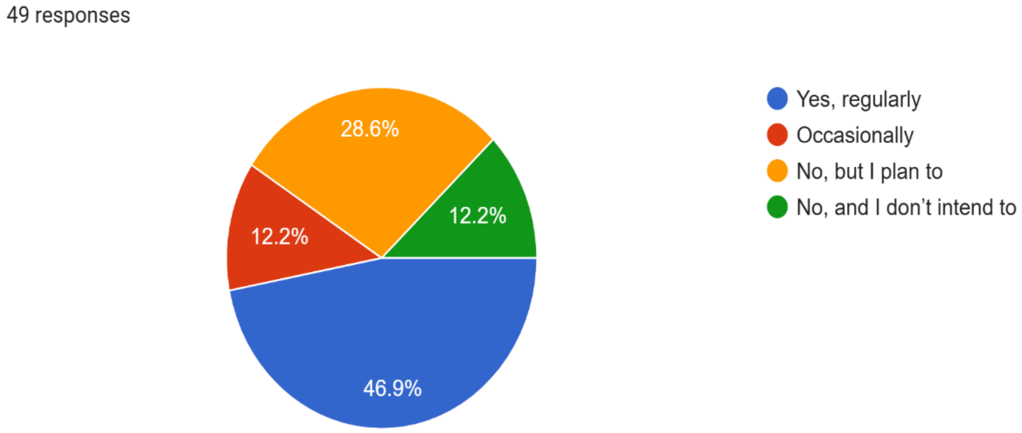
**Table 1: How familiar are you with the risks children face online?**

| Type | Number of respond | Percentage |
|---|---|---|
| Very familiar | 26 | 52% |

| | | |
|---|---|---|
| Somewhat Familiar | 14 | 28% |
| Heard of it but don’t know much | 07 | 14% |
| Not familiar at all | 03 | 6% |

**Interpretation :**

The data shows that a combined 80% of respondents are at least somewhat aware of the risks children face online. This reflects a relatively high level of awareness among youth, which is encouraging for future efforts in online child safety advocacy. However, the existence of a knowledge gap (20%)—especially the 14% who have minimal understanding—highlights the need for more targeted education and awareness campaigns to ensure all individuals are well-informed and equipped to protect children in the digital space.



**Parental Practices & Technology Use**

**Table 2: Do you use any parental control tools or monitoring apps to supervise your child's online activities?**

| Technology Use | Number of respond | Percentage |
|---|---|---|
| Yes, regularly | 23 | 46% |
| Occasionally | 06 | 12% |
| No, but I plan to | 14 | 28% |
| No,and I don’t intend to | 06 | 12% |

**Interpretation:**

The data shows that 58% of respondents are currently using parental controls either regularly or occasionally, which is encouraging in terms of immediate protective measures. Additionally, with 28% planning to adopt them, there is a strong indication of growing interest in tech-based safety tools. However, the 12% who reject their use entirely may require awareness programs that emphasize the importance and benefits of digital supervision in preventing online risks for children.

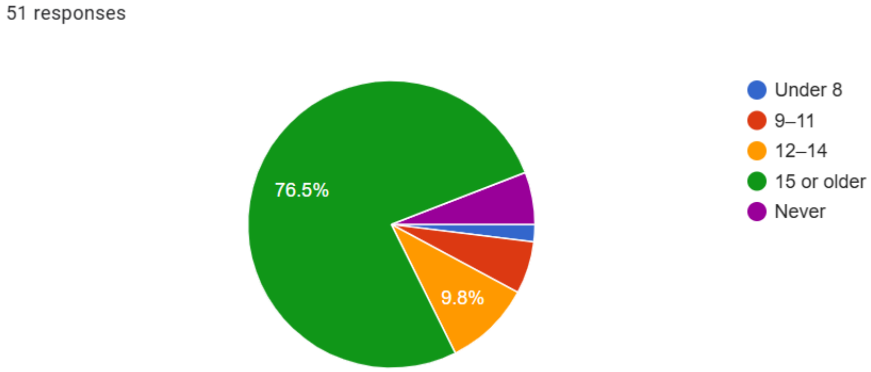


**Table3: At what age do you think it is appropriate for a child to have their own smartphone or personal device?**

| Age | Number of respond | Percentage |
|---|---|---|
| 9-11 | 05 | 8% |
| 12-14 | 04 | 9% |
| 15 or older | 38 | 76% |
| Never | 04 | 5% |

**Interpretation:**

The dominant view (76%) favoring age 15 or older reflects a general preference for delaying personal device ownership until adolescence, when children are presumed to have greater digital literacy and self-regulation. The minimal support for earlier ages underscores a widespread concern about the early introduction of technology and its potential negative effects. This highlights the importance of parental guidance, digital literacy education, and gradual exposure to technology under supervision for younger children.

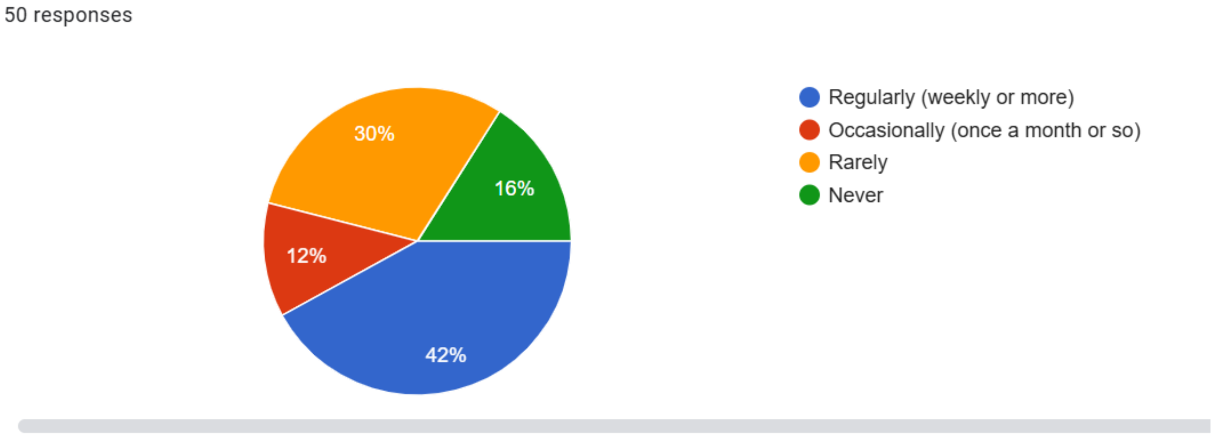
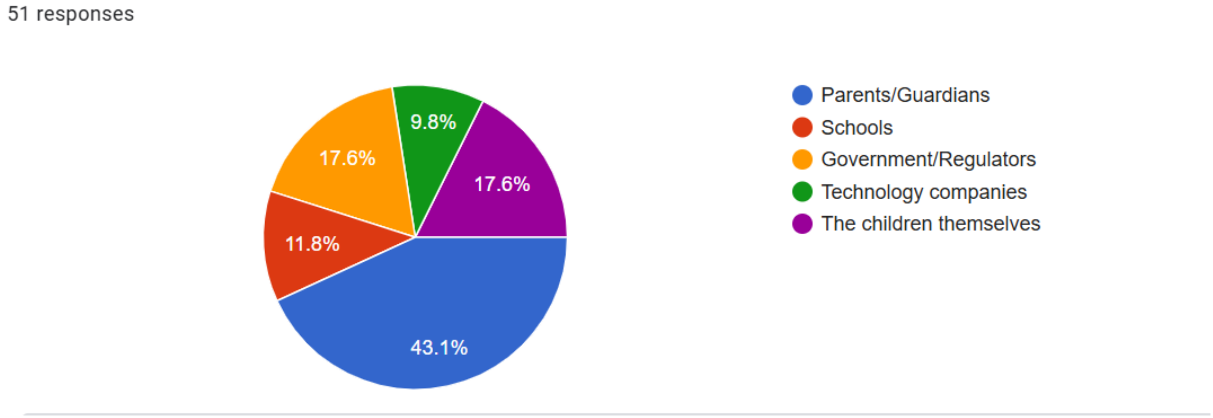


**Table4: How often do you talk to your child(ren) about safe internet practices?**

| Catagories | Number of respond | percentage |
|---|---|---|
| Regularly | 21 | 42% |
| Occasionally | 06 | 12% |
| Rarely | 15 | 30% |
| Never | 08 | 16% |

**Interpretation:**

Regular communication is a cornerstone of digital safety. The presence of any respondents in the "rarely" or "never" categories highlights a critical gap in preventive education at home. Efforts should be made to educate parents about the importance of frequent and age-appropriate conversations with children regarding online behavior, privacy, cyberbullying, and digital responsibility.



**Opinions & Recommendations**

**Table5: In your opinion, who holds the greatest responsibility for protecting children online?**

| Catagories | Number of respond | percentage |
|---|---|---|
| Parents/guardians | 21 | 43% |
| Schoools | 05 | 11% |
| Government | 08 | 17% |
| Technology companies | 05 | 9% |
| The children themselves | 07 | 17% |

**Interpretation:**

This question highlights that online child protection is a shared responsibility, but public perception often places the greatest burden on parents and guardians, as they have direct influence over children's behavior and online access. However, the involvement of schools, government bodies, and tech companies is also considered crucial, pointing to the need for a multi-stakeholder approach to online safety. Policies, education, and technology must all work together to create a secure digital environment for children.

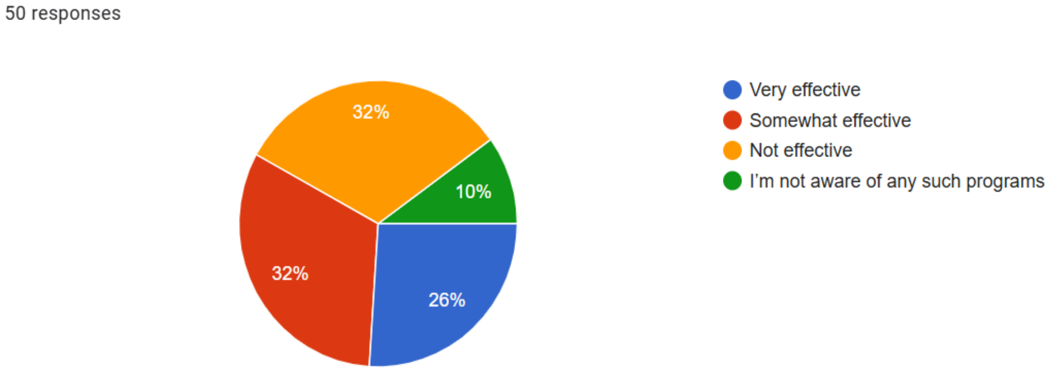


**Table6: How effective do you believe current school programs are in educating children about online safety?**

| Catagories | number of respond | percentage |
|---|---|---|
| Very effective | 12 | 26% |
| Somewhat effective | 16 | 32% |
| Not effective | 16 | 32% |
| I'm not aware | 05 | 10% |

**Interpretation:**

The presence of responses across all categories shows a mixed perception of school program effectiveness. While some schools may be delivering impactful digital safety education, others may lack the resources, training, or emphasis to do so effectively. The lack of awareness among some respondents also highlights a need for better outreach and visibility of existing programs. Overall, the findings suggest that more consistent, comprehensive, and clearly communicated efforts are needed in schools to ensure all children receive essential guidance on navigating the online world safely.

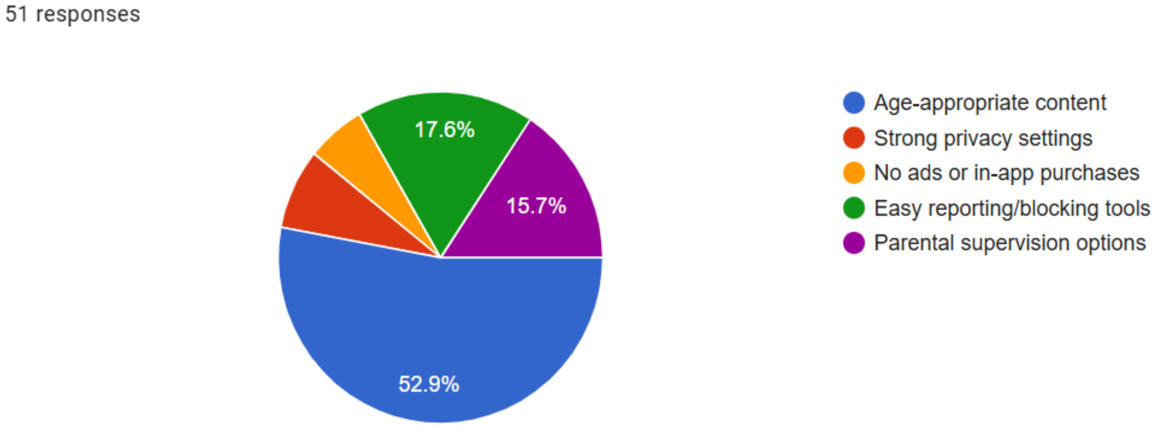


**Table7: What features do you think are essential in apps/websites designed for children?**

| Categories | Number of respond | Percentage |
|---|---|---|
| Age-appropriate content | 26 | 53% |
| Strong privacy settings | 08 | 8% |
| No ads or in-app purchases | 08 | 6% |
| Easy reporting/blocking tools | 09 | 17% |
| Parentals supervision options | 07 | 16% |

**Interpretation:**

The responses reveal a comprehensive understanding of child-centered digital safety, where both content control and interaction safety are equally valued. The strong emphasis on privacy, ad-free experiences, and parental oversight suggests that respondents want platforms not only to entertain or educate but also to protect and respect children's rights and vulnerabilities. Developers should take these insights seriously to design ethical, secure, and child-friendly digital environments..

50 responses

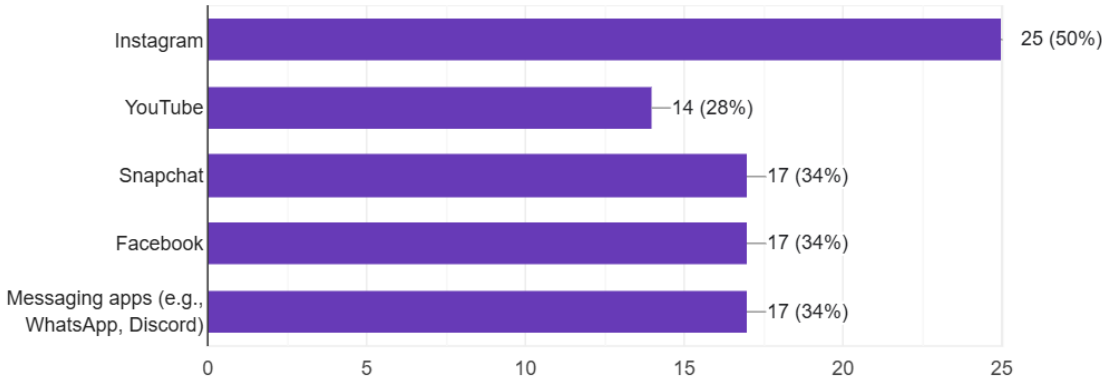


**Table8: Which platforms do you believe are most risky for children?**

| App | Number of respond | Percentage |
|---|---|---|
| Instagram | 25 | 50% |
| You Tube | 14 | 28% |
| Snapchat | 17 | 34% |
| Facebook | 17 | 34% |
| WhatsApp | 17 | 34% |

**Interpretation:**

The data shows that Instagram is perceived as the highest-risk platform, likely due to its popularity among youth and lack of content controls. The consistently high risk perception across multiple platforms (Snapchat, Facebook, WhatsApp) highlights that no single app is considered fully safe, and each poses unique challenges.

51 responses

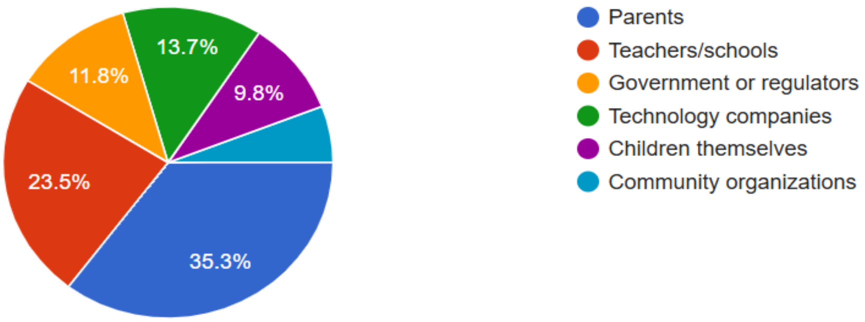


**Table9: Who should take the lead in educating children about online safety?**

| Categories | Number of respond | Percentages |
|---|---|---|
| Parents | 17 | 35% |
| Teachers | 11 | 23% |
| Government | 05 | 12% |
| Technology companies | 07 | 13% |
| Children themselves | 05 | 10% |
| Community organisation | 04 | 9% |

**Interpretation:**

The variety of responses emphasizes that online safety education is a shared responsibility. However, the majority likely expect parents and schools to take the lead, supported by policy-makers, tech companies, and community efforts. This points to the need for a collaborative, multi-stakeholder approach, where every group plays a defined and proactive role in safeguarding children in the digital world.

## FINDINGS

The findings from the survey of 60 undergraduate students in Delhi NCR reveal that while there is a relatively high level of awareness (80%) about online risks faced by children, significant gaps persist in practical engagement and education. A majority believe that children should not own personal devices until age 15 or older, reflecting concerns over early exposure to online threats. Although 58% of respondents use parental controls, nearly half rarely or never discuss online safety with children, indicating a lack of consistent communication. Most respondents view parents as primarily responsible for protecting children online, though schools, government, and tech companies are also seen as important contributors. Instagram is perceived as the riskiest platform, and age-appropriate content is considered the most essential feature for child-focused apps and websites. Opinions on the effectiveness of school programs are mixed, with many unaware of existing initiatives, underscoring the need for a more coordinated, multi-stakeholder approach to ensure children's online safety through education, supervision, and safer digital environments.

The analysis of primary data collected from 60 undergraduate students in Delhi NCR reveals a nuanced understanding of the challenges and responsibilities associated with protecting children online. A significant majority (80%) of respondents are at least somewhat aware of the risks children face on the internet, such as cyberbullying, exposure to inappropriate content, and online predators. However, a notable 20% still demonstrate limited or no awareness, indicating a gap that calls for targeted educational efforts. In terms of supervision, 58% of respondents reported using parental control tools either regularly or occasionally, while 28% plan to use them in the future—reflecting a growing interest in tech-based safety measures. Yet, 42% of respondents rarely or never communicate with children about online safety, which is concerning given the importance of ongoing guidance. When asked about the appropriate age for device ownership, an overwhelming 76% believe children should be 15 or older before having their own smartphone, reflecting a cautious approach toward early digital independence. Most respondents (43%) place the primary responsibility for online child protection on parents, though schools (11%), the government (17%), technology companies (9%), and even children themselves (17%) are also seen as playing important roles. School programs received mixed reviews—only 26% found them very effective, while 32% found them ineffective and 10% were unaware of any programs, indicating a need for more visible and consistent efforts in digital safety education. Instagram was perceived as the most risky platform (50%), followed by Snapchat, Facebook, and WhatsApp (each 34%), and YouTube (28%). Respondents identified age-appropriate content (53%) as the most essential feature for child-friendly digital platforms, alongside reporting/blocking tools and parental supervision options. Overall, the findings emphasize the need for a multi-stakeholder approach, with a stronger focus on awareness, communication, school-based education, policy regulation, and safer platform design to comprehensively protect children in the digital world.

When asked about the appropriate age for smartphone ownership, 76% of respondents believe children should be 15 years or older before having personal access to digital devices, reflecting a strong consensus on delaying digital independence until a more mature age. Opinions on who should take the lead in protecting children online were also telling: 43% placed the primary responsibility on parents or guardians, but a significant number also recognized the roles of schools (11%), government/regulatory bodies (17%), technology companies (9%), and even children themselves (17%), reinforcing the idea that online safety is a shared responsibility. School-based education programs were evaluated with mixed responses—only 26% found them very effective, 32% somewhat effective, and another 32% said they were not effective at all. Notably, 10% were unaware of any such programs, indicating a lack of visibility and possibly inconsistent implementation across schools.

In terms of digital platform risk, Instagram was rated the most risky (50%), followed by Snapchat, Facebook, and WhatsApp (each 34%), and YouTube (28%). This suggests that social media and messaging apps—particularly those lacking robust content moderation or offering private, disappearing messages—are seen as environments where children are highly vulnerable. As for safety features on child-focused apps and websites, age-appropriate content was the top priority (53%), followed by easy reporting and blocking tools (17%), parental supervision options (16%), and strong privacy settings and ad-free environments receiving less emphasis (8% and 6%, respectively). These responses indicate a clear public demand for digital spaces that are not only engaging for children but also secure, transparent, and easy to monitor.

In conclusion, the findings point to the urgent need for a **multi-level strategy** involving **parental engagement, educational reform, stronger digital platform accountability, and government policy support** to build a safer digital ecosystem for children. While awareness among youth is relatively high, practical application through communication, school programs, and consistent digital parenting is still lacking

## Conclusion

The study on protecting children online, based on responses from 60 undergraduate students in Delhi NCR, reveals both encouraging awareness and noticeable gaps in practical action. Most respondents (80%) demonstrate a fair to strong understanding of online risks children face, such as exposure to inappropriate content, cyberbullying, and online predators. However, the lack of in-depth knowledge among 20% of respondents indicates the ongoing need for awareness-building efforts, especially among future parents and educators. Parental engagement in digital supervision is moderate, with 58% using parental controls and another 28% intending to adopt such tools, yet nearly half of respondents do not engage in regular conversations with children about online safety—an essential aspect of prevention and guidance.

A significant 76% of respondents agree that children should only be given personal digital devices at age 15 or older, reflecting a cautious and responsible attitude toward early digital exposure. The majority (43%) view parents as the key figures in ensuring online safety, but the data also highlights a broader understanding that schools, governments, tech companies, and children themselves must all contribute to creating a safe digital ecosystem. Perceptions of school program effectiveness are mixed, with a notable proportion of respondents unaware of any such initiatives, pointing to a need for more standardized and visible school-based digital literacy education.

Platforms such as Instagram, Snapchat, Facebook, and WhatsApp are widely seen as risky due to their content, user anonymity, and lack of adequate child safety features. Respondents prioritize age-appropriate content, blocking/reporting tools, and parental supervision as the most essential features for child-friendly apps and websites. Collectively, these findings underscore the importance of a multi-stakeholder approach—where parents, educators, policy-makers, technology providers, and communities work together to ensure that children are not only protected but also empowered to navigate the online world safely and responsibly. Strengthening digital literacy, enhancing communication, and building safer digital platforms are crucial next steps in addressing the evolving challenges of online child safety.

## Limitations of the Study

While this study provides meaningful insights into the awareness, attitudes, and practices related to online child safety among undergraduate students in Delhi NCR, it is important to recognize several limitations that may influence the validity, reliability, and generalizability of the findings. These limitations are outlined below:

**1. Limited Sample Size**

The study was conducted with a sample size of only 60 respondents. Although this number provides a preliminary understanding of perceptions surrounding child online safety, it is relatively small when considering the large and diverse population of Delhi NCR. A larger sample size would have improved the statistical accuracy and reliability of the findings and allowed for more nuanced subgroup analyses based on age, gender, or educational background.

**2. Homogeneous Respondent Group (Undergraduate Students)**

All participants in the study were undergraduate students. While this demographic is relevant—since they are likely future parents, educators, or tech users—they may lack direct experience in parenting or supervising children. As a result, their responses may reflect hypothetical opinions rather than practical knowledge or actions. This limits the study's applicability to real-world parenting behaviors and decision-making regarding child safety online.

**3. Geographical Limitation**

The research is geographically confined to Delhi NCR, which is an urban region with relatively better access to education, technology, and digital infrastructure. This urban-centric focus may not accurately represent the views or digital parenting practices of individuals in rural or semi-urban areas, where awareness levels, access to digital tools, and exposure to internet risks can differ significantly. Therefore, the results may not be generalizable to all parts of India.

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

The study employed structured questionnaires as the primary data collection tool. While efficient, this method relies heavily on the honesty, understanding, and self-awareness of the respondents. Responses may be influenced by **social desirability bias** (providing answers that seem socially acceptable) or **recall bias** (inaccurate memory of past behavior), which can affect the authenticity of the data, especially in sensitive areas such as parental control usage or online safety discussions.

**5. Lack of Qualitative Insights**

The use of close-ended survey questions allowed for statistical analysis but limited the depth of exploration into individual experiences, motivations, and reasoning. Qualitative methods such as interviews or focus group discussions could have offered richer insights into how respondents perceive online threats, make decisions, or emotionally respond to digital risks affecting children. Without this, the study lacks the emotional and contextual dimensions of the issue.

**6. Cross-Sectional Nature of the Study**

This research provides a snapshot of respondents' attitudes and behaviors at a single point in time. However, perceptions and practices regarding online child safety are dynamic and can change due to evolving technologies, new threats, public awareness campaigns, or personal experiences. A longitudinal study would better capture trends over time and offer insights into how and why attitudes or behaviors shift.

**7. No Direct Input from Parents or Children**

Although the study focuses on online safety for children, it does not include responses from actual parents or children—the primary stakeholders. Including these groups would have added direct experiential perspectives and made the findings more grounded and relevant to real-life family dynamics and challenges.

**Summary**

while the study successfully identifies general awareness levels and public attitudes toward online child protection among undergraduate students, it is subject to several methodological and contextual limitations. Future research should aim to include a larger and more diverse sample, incorporate qualitative methods, involve parents and children directly, and consider regional diversity to provide a more holistic and accurate understanding of the issue.

## SUGGESTIONS

Based on the findings and limitations of this study, several actionable suggestions can be proposed to strengthen online child safety. These recommendations aim to support parents, educators, policymakers, and technology developers in fostering a safer digital environment for children. The suggestions are organized across key stakeholders:

**1. For Parents and Guardians**

- Regular Communication: Parents should initiate regular, age-appropriate conversations with their children about internet safety. Topics should include cyberbullying, privacy, safe browsing habits, and how to report harmful content. Open communication builds trust and encourages children to seek help when needed.

- Use of Parental Control Tools: Parents should actively use and stay updated on available parental control software and monitoring tools. These tools can help filter inappropriate content, monitor screen time, and track online activities.

- Set Digital Boundaries: Establish clear rules for screen time, device usage, and app installations. Co-creating a "digital agreement" with children can foster responsibility and transparency.

- Lead by Example: Children often mimic adult behavior. Parents should model healthy online habits, such as respectful communication, balanced screen use, and mindful content consumption.

**2. For Educational Institutions**

- Incorporate Digital Safety into the Curriculum: Schools should integrate digital citizenship and online safety education into the core curriculum from an early age. Topics should include online ethics, responsible content sharing, and recognizing misinformation.

- Train Teachers: Provide teachers with professional training on cyber safety so they can effectively educate and support students. Teachers should be equipped to identify signs of cyberbullying or online abuse and know how to respond.

- Engage Parents through Workshops: Schools should organize regular workshops or webinars for parents to inform them about digital risks, safe practices, and the latest trends in technology use among children.

- Create Safe Reporting Mechanisms: Establish anonymous, accessible reporting systems in schools for students to report online harassment, abuse, or suspicious activities.

**3. For Government and Policy Makers**

- Mandate Online Safety Education: Enforce policies requiring all schools to implement structured digital safety education programs, including online behavior, legal rights, and mental health impacts.

- Launch Awareness Campaigns: Government-led campaigns should promote public awareness about child online safety through TV, social media, and community centers, especially targeting rural and underserved areas.

- Regulate Child-Oriented Digital Spaces: Strengthen regulations on platforms targeting children by enforcing stricter content controls, advertising standards, and data privacy laws in line with global frameworks like GDPR and COPPA.

- Support Research and Data Collection: Encourage and fund academic research on children's digital behavior to inform future policies and protective measures.

**4. For Technology Companies**

- Design with Safety First: Developers should integrate child protection features such as age verification, content filters, time-limit options, and reporting tools by default in apps and websites used by or accessible to children.

- Ensure Transparency and Accountability: Platforms must be transparent about how they collect, use, and store children's data, and should offer clear opt-out or privacy customization features for parents.

- Limit Ads and In-App Purchases: Children's apps should avoid manipulative advertising and remove access to in-app purchases without adult consent to prevent exploitation.

- Collaborate with Experts: Work closely with child psychologists, educators, and legal experts when designing child-friendly platforms to ensure developmental appropriateness and legal compliance.

**5. For Community Organizations and NGOs**

- Run Digital Literacy Programs: NGOs can play a key role by conducting training sessions in schools and community centers, particularly in low-income and rural areas where digital literacy is low.

- Provide Support Services: Offer counseling, helplines, and support networks for children who have faced online abuse, and work with parents to create recovery and prevention strategies.

- Promote Peer Education: Initiatives that empower teens to teach younger children about digital safety have been shown to be effective, as children often relate better to peers than adults.

**6. For Children and Adolescents**

- Encourage Self-Awareness and Responsibility: Children should be educated and encouraged to take responsibility for their online behavior, including respecting others, protecting their privacy, and recognizing unsafe situations.
- Promote Digital Literacy Early: Teach children how to critically evaluate online content, recognize misinformation, and understand the permanence of digital footprints.
- Support Peer Dialogue: Children should feel comfortable discussing their online experiences with peers and adults, contributing to a culture of openness and shared learning.

## BIBLIOGRAPHY

**1.** UNICEF. (2021). *Child Online Protection: Protecting children in the digital world*. Retrieved from https://www.unicef.org

**2.** Livingstone, S., & Helsper, E. (2007). *Gradations in digital inclusion: Children, young people and the digital divide*. New Media & Society, 9(4), 671–696.

**3.** National Crime Records Bureau (NCRB). (2023). *Cyber Crime in India*. Ministry of Home Affairs, Government of India.

**4.** International Telecommunication Union (ITU). (2020). *Guidelines on Child Online Protection*. Retrieved from https://www.itu.int

**5.** Common Sense Media. (2022). *The Common Sense Census: Media Use by Tweens and Teens*. Retrieved from https://www.commonsensemedia.org

**6.** Ministry of Electronics & Information Technology (MeitY), Government of India. (2021). *Digital Safety for Children and Adolescents*. Retrieved from https://www.meity.gov.in

**7.** Patchin, J. W., & Hinduja, S. (2018). *Cyberbullying: Identification, Prevention, and Response*. Cyberbullying Research Center. Retrieved from https://cyberbullying.org

**8.** Ofcom (UK). (2023). *Children and Parents: Media Use and Attitudes Report*. Retrieved from https://www.ofcom.org.uk

**9.** Kapoor, K., & Sharma, M. (2022). *Digital Parenting in India: Challenges and Strategies*. International Journal of Child and Adolescent Health, 15(2), 89–98.

**10.** Google Safety Center. (n.d.). *Tips for Families: Keeping Your Family Safer Online*. Retrieved from https://safety.google/families/