Journal of Advances in Developmental Research (IJAIDR)

E-ISSN: 0976-4844 ● Website: www.ijaidr.com ● Email: editor@ijaidr.com

Empowering Digital Learners: From Vulnerability to Resilience

Dr. Sourav Maity

Independent Researcher
West Bengal, India

Abstract:
The rapid expansion of digital infrastructure in Indian schools, accelerated significantly by the COVID-19 pandemic, has created a critical gap between technological access and online safety preparedness among school-going children. While India's National Education Policy (NEP) 2020 promotes digital literacy and computational thinking as essential skills, it is argued that these cannot be effectively pursued without a parallel and structured framework for cyber security education. This paper identifies and categorises the primary online threats faced by students in India today, including content-based risks such as misinformation and harmful material, contact-based risks including cyberbullying and online grooming, and infrastructure risks arising from weak data protection practices in school networks. An evaluation of existing legal instruments, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, reveals significant gaps in their practical applicability to school environments. Addressing these regulatory and structural systemic gaps is fundamental to empowering digital learners across the nation. In response, this paper outlines an actionable roadmap designed to transition the educational landscape from vulnerability to resilience by replacing purely restrictive rules with proactive student behaviours. The first pillar suggests the integration of age-appropriate cyber safety education across all grade levels. The second advocates for the deployment of robust technical safeguards within school infrastructure. The third emphasises capacity building among teachers and parents as essential stakeholders in student online safety. Implementation challenges, including the urban-rural digital divide, teacher workload, and cultural barriers to reporting, are also examined. The paper concludes with targeted policy recommendations for NCERT, CBSE, and State Education Boards to institutionalise cyber safety as a foundational component of modern school education in India.

Keywords: Cyber Safety, Digital Literacy, NEP 2020, Cyberbullying, School Cyber Security, Digital Citizenship, Data Protection.

INTRODUCTION

Over the past few years, Indian schools have gone through a massive shift towards digital learning. The COVID-19 pandemic pushed this change even faster. Today, millions of students attend online classes, use digital libraries, and study in smart classrooms. Technology is now a central part of how children learn in India. Indian schools are rapidly adopting online and hybrid learning, but students' cyber safety knowledge and protections lag far behind this digital expansion. Research from India and other countries points to low awareness, high exposure to online risks, and the need for structured, curriculum-level cyber

safety frameworks (Rahman et al., 2020). When schools have invested in hardware and internet connections, there has been far less attention given to one important question: are students safe online? Children today are spending more time on the internet than ever before, but most of them have not been taught how to protect themselves from online dangers. This gap between digital access and digital safety has become a serious concern. India's National Education Policy (NEP) 2020 rightly promotes digital literacy and computational thinking as key skills for the future. However, it is important to recognise that digital literacy is incomplete without cyber security. A student who knows how to use a computer but does not know how to stay safe online is like a driver who knows how to start a car but has never been taught traffic rules. The two must go together. This paper argues that Indian schools need a clear, practical, and well-funded cyber safety policy framework that protects students both inside and outside the classroom.

THE PROBLEM: WHAT THREATS DO STUDENTS FACE ONLINE?

Students in India today face a wide range of online threats. These can be grouped into three broad categories:

Content Based Risks: Harmful, Violent, and Extremist Material

Children's everyday internet use exposes them to violent and sexual content, misinformation, and extremist material, often without them actively seeking it (Nienierza et al., 2019). Research shows these exposures are common, emotionally upsetting, and can shape attitudes and behaviours over time (Livingstone et al., 2014). Many children are exposed to harmful content online without even looking for it (Ayyash et al., 2023). This includes:

- Age-inappropriate material such as graphic violence or adult content
- Misinformation and fake news, which can mislead young minds
- Radicalising content that promotes extremist views

Contact Based Risks:

These risks involve harmful interactions with other people online:

- Cyberbullying, where students are mocked, threatened, or harassed by peers online (Zhu et al., 2021).
- Online grooming, where adults with bad intentions build false trust with children (Sharma et al., 2021).
- Phishing scams, where students are tricked into sharing personal information (Chiner et al., 2025).
- Identity theft, which can have long-lasting consequences even for minors (Bhat, C. S. 2018).

Infrastructure Risks:

In rural or under-resourced Indian contexts, infrastructure and training gaps are particularly severe, leaving schools highly vulnerable to attacks and data misuse (Alier et al., 2021). Many schools in India use shared networks and devices that are not properly secured. Student records, attendance data, and personal details are often stored without proper data protection measures. Weak security on school servers can lead to data leaks, putting students and their families at risk.

Behavioural and Psychological Risks:

The unregulated use of digital devices has led to a sharp rise in screen and gaming addiction among students (Alter, A. 2017). Compulsive engagement with video games and social media algorithms often results in severe psychological and physical impacts, including chronic sleep deprivation, anxiety, declining academic performance, and social withdrawal. Study shows 16%–19% of adolescents are

addicted to online gaming which was strongly associated with depression, anxiety, stress, and psychological distress (Saquib et al., 2017).

These are not distant or unlikely problems. Cases of cyberbullying among school students have been reported across Indian cities, and there is growing concern among educators and parents about the lack of structured guidance on online safety.

WHAT DOES THE LAW SAY? EXISTING RULES AND THEIR LIMITATIONS

India does have some laws related to cyber safety, but they are not fully equipped to address the specific needs of school-going children.

The IT Act, 2000:

The Information Technology Act, 2000, is the main law governing cyber offences in India. It covers crimes like hacking, spreading harmful content, and online fraud. However, this law was written before social media, smartphones, and digital classrooms became widespread. It does not specifically address the protection of minors in online educational settings, and its language is too technical for schools to act on.

The Digital Personal Data Protection (DPDP) Act, 2023:

This is a significant step forward. The DPDP Act, 2023, specifically restricts the collection and processing of data belonging to children. Schools and third-party app providers cannot collect a child's personal information without verified parental consent. Schools must now take this law seriously and review how they store and handle student data. Many schools are still not fully compliant with these requirements.

NCERT and CBSE Guidelines:

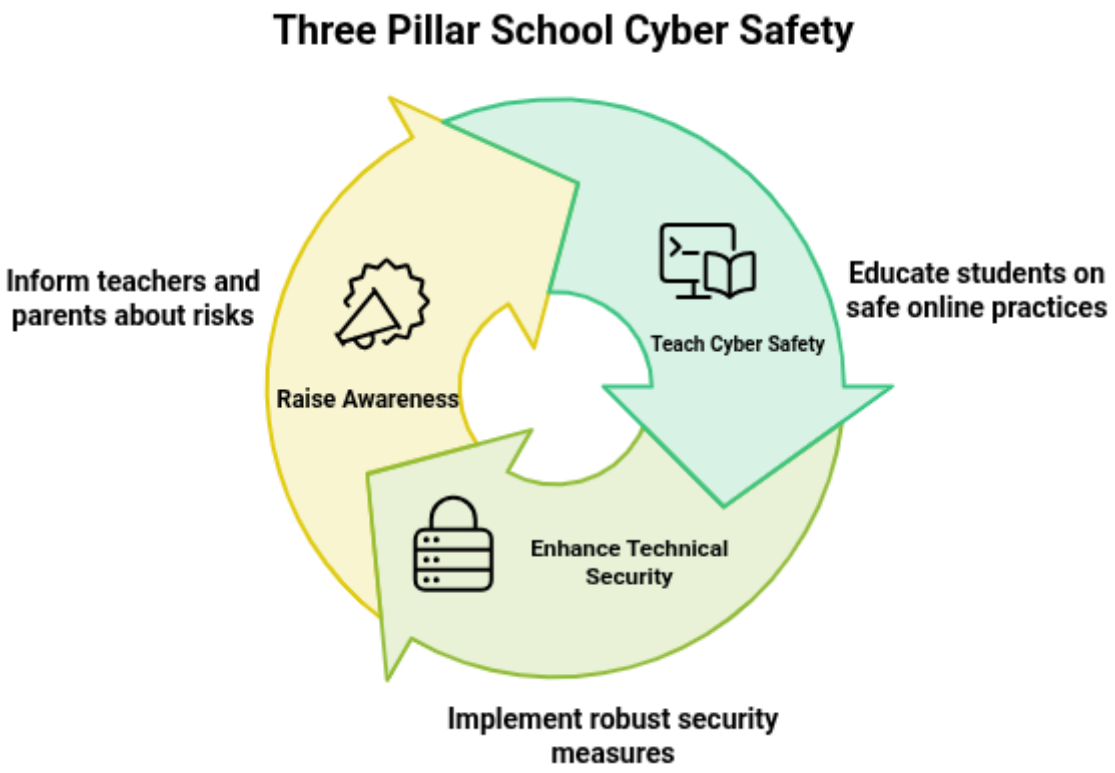
The National Council of Educational Research and Training (NCERT) and the Central Board of Secondary Education (CBSE) have published some cyber safety material in the past, including handbooks and chapters in textbooks. While these efforts are appreciated, they are not enough. The material is often treated as a one-time lesson rather than a continuous, integrated part of the curriculum. There is no unified national policy that tells schools exactly what they must do to keep students safe online. In short, the legal and policy framework exists in pieces, but it has not been stitched together into a complete, school-ready system.

A ROADMAP TRANSITIONING EDUCATION FROM VULNERABILITY TO RESILIENCE

To achieve comprehensive cyber safety, the following three-pillar roadmap addresses the problem across three distinct dimensions

Pillar A: Teaching Cyber Safety in the Classroom

Currently, cyber safety is often discussed in a one-off seminar or a single chapter in a textbook. This approach is not effective. It is recommended that age-appropriate cyber safety education be made a regular part of the school curriculum for secondary and higher secondary school students (Uramova et al., 2024). For secondary students (Classes 9 & 10), lessons could focus on simple rules, such as not sharing personal information with strangers online and telling a trusted adult if something feels wrong. For higher secondary school students (11 & 12), the focus could shift to recognising cyberbullying, understanding privacy settings, identifying fake news and more advanced topics such as data protection, digital rights, and responsible use of social media should be covered. This approach is often called ‘Digital Citizenship’ education. It teaches children not just how to use technology, but how to use it wisely, ethically, and safely (Althibyani, H. A. 2023).



Pillar B: Making Schools Technically Safer

Schools must deploy robust technical safeguards to protect students while they use school networks and devices. This includes:

- Enterprise-grade firewalls that block known harmful websites (Saglam et al., 2023).
- Content filtering software that restricts access to age-inappropriate material (Lester, T. 2018)
- Encrypted storage for student data to prevent unauthorised access (Bae, S. M. 2021).
- Anonymous reporting systems, so that students can report cyberbullying or online harassment without fear of being identified (Chiner, E. 2025).

Schools must conduct regular security audits of their networks to identify and fix vulnerabilities. Those unable to afford these audits independently should receive state government support through centralized IT services

Pillar C: Building Awareness Among Teachers and Parents

Technology alone cannot solve the problem; the human ecosystem surrounding students matters just as much. Essential steps include:

- All teachers receive regular training to recognise warning signs of cyber-related distress in students, such as sudden changes in behaviour, a drop in grades, or anxiety related to device use (Ayyash et al., 2024).
- Schools hold at least one mandatory awareness workshop for parents each academic year, covering topics like safe app usage, parental controls, and how to have open conversations with children about online experiences (Lester, T. 2018).
- A school cyber safety coordinator role is important, where a trained staff member is responsible for monitoring online safety and responding to incidents (Bickham, D, 2020).

Parents are especially important because the majority of a child's internet use happens at home, not at school. Equipping parents with the right knowledge is just as important as training teachers.

CHALLENGES IN PUTTING THIS INTO PRACTICE

Implementing a national cyber safety framework across a country as vast and diverse as India naturally presents significant operational challenges that require realistic assessment.

The Urban-Rural Divide:

Urban schools often have better ICT infrastructure and institutional support, while rural schools face poor internet, few devices, and outdated software, which directly limits cyber safety training and practice (Mustafa, F, 2024). A school in Mumbai or Bengaluru may have a dedicated IT department, reliable internet, and smart classrooms. A school in a rural district of West Bengal or Jharkhand may have limited electricity and little to no internet connectivity. Any national policy must account for this reality and provide scaled-down, practical alternatives for schools with fewer resources. A one-size-fits-all approach will not work.

Teacher Workload, Digital Skills, and Support:

Teachers are increasingly using digital tools but often lack basic cybersecurity know-how, especially in rural and semi-urban areas. Many have low awareness of passwords, phishing, and device safety, and schools rarely provide structured incident response or clear protocols (Rawal, D. M, 2024). On the other hand, Indian teachers are already overworked. Asking them to take on additional responsibilities related to cyber safety oversight, without proper training or compensation, is unfair and unlikely to succeed. Any new policy must come with dedicated training programmes and, where possible, a reduction in other administrative burdens.

Cultural and Reporting Barriers:

In many Indian households, there is still a stigma around children using the internet. When a student faces cyberbullying or online harassment, they are often afraid to report (Ondruskova, D., & Pospisil, R. 2023) because they fear their parents will take their phone or internet access away as a punishment. Schools and parents need to work together to create an environment where children feel safe speaking up about online problems without fear of being blamed or punished (Rajbhandari, J., & Rana, K., 2022).

CONCLUSION

Cyber security education in schools is no longer optional. As India continues its journey towards becoming a digitally advanced nation, the safety of its youngest citizens online must be treated as a priority, not an afterthought. The three-pillar framework proposed in this paper focused on curriculum, technical safeguards, and stakeholder awareness offers a practical and comprehensive path forward. It is neither overly complex nor beyond the reach of the Indian education system, provided there is political will and institutional support.

The following steps are highly encouraged for bodies such as NCERT, CBSE, and state education departments to implement:

- Develop and mandate a graded cyber safety curriculum for all school levels.
- Issue clear compliance guidelines for schools under the DPDP Act, 2023.
- Allocate dedicated funding for technical infrastructure in government schools.
- Launch a national teacher training programme on cyber safety and digital wellness.

● Create a student-friendly, anonymous, online grievance reporting portal at the national level.

Ultimately, the goal is simple: every child in India should be able to learn, explore, and grow in the digital world without fear. Achieving that goal requires schools, governments, parents, and communities to work together with urgency and purpose.

REFERENCES:

1. Alier, M., Guerrero, M. J. C., Amo, D., Severance, C., & Fonseca, D. (2021). *Privacy and E-Learning: A Pending Task. Sustainability*. https://doi.org/10.3390/su13169206
2. Alter, A. (2017). *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin Press.
3. Althibyani, H. A., & Alzahrani, A. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*. https://doi.org/10.3390/su151511512
4. Ayyash, M., Alsboui, T. A. A., Alshaikh, O., Inuwa-Dutse, I., Khan, S., & Parkinson, S. (2024). Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain. *IEEE Access*, 12, 86596-86617. https://doi.org/10.1109/access.2024.3416045
5. Bae, S. M. (2021). The relationship between exposure to risky online content, cyber victimization, perception of cyberbullying, and cyberbullying offending in Korean adolescents. *Children and Youth Services Review*, 123, 105946. https://doi.org/10.1016/j.childyouth.2021.105946
6. Bhat, C. S. (2018). Cyber bullying and online predatory grooming among school students: A study. *Journal of the Indian Academy of Applied Psychology*, 190-193.
7. Bickham, D. (2020). Evaluating a Middle-School Digital Citizenship Curriculum (Screenshots): Quasi-Experimental Study. *JMIR Mental Health*, 8. https://doi.org/10.2196/26197
8. Chiner, E., Gómez-Puerta, M., Mengual-Andrés, S., & Merma-Molina, G. (2025). Teacher and School Mediation for Online Risk Prevention and Management: Fostering Sustainable Education in the Digital Age. *Sustainability*. https://doi.org/10.3390/su17083711
9. Computer Science Teachers Association. (2017). *K-12 computer science framework*. CSTA.
10. Government of India. (2000). *Information Technology Act, 2000 (amended 2008)*. Ministry of Law and Justice.
11. Government of India. (2012). *Protection of Children from Sexual Offences Act, 2012 (amended 2019)*. Ministry of Law and Justice.
12. Government of India. (2013). *National Cyber Security Policy 2013*. Department of Electronics and Information Technology.
13. Government of India. (2020). *National Education Policy 2020*. Ministry of Human Resource Development.
14. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Electronics and Information Technology.
15. Internet and Mobile Association of India. (2022). *India internet report 2022*. IAMAI.
16. ITU. (2020). *Guidelines for industry on child online protection*. International Telecommunication Union.
17. Lester, T. (2018). *An Investigation on Cyber Safety Awareness Among Teachers and Parents*. *(Note: Placed once to remove the duplicate entry from your original list)*

18. Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age.. Journal of child psychology and psychiatry, and allied disciplines, 55 6, 635-54 . https://doi.org/10.1111/jcpp.12197
19. Mustafa, F. (2024). The challenges and solutions of technology integration in rural schools: A systematic literature review. *International Journal of Educational Research*. https://doi.org/10.1016/j.ijer.2024.102380
20. Nienierza, A., Reinemann, C., Fawzi, N., Riesmeyer, C., & Neumann, K. (2019). Too dark to see? Explaining adolescents' contact with online extremism and their ability to recognize it. Information, Communication & Society, 24, 1229 - 1246. https://doi.org/10.1080/1369118x.2019.1697339
21. Ondruskova, D., & Pospisil, R. (2023). The good practices for implementation of cyber security education for school children. *Contemporary Educational Technology*. https://doi.org/10.30935/cedtech/13253
22. Rahman, N. A., Sairi, I. H., Zizi, N., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. International Journal of Information and Education Technology. https://doi.org/10.18178/ijiet.2020.10.5.1393
23. Rawal, D. M. (2024). Mapping of school teachers' digital competency in the context of digital infrastructure: a systematic review and empirical study of India. *Journal of Professional Capital and Community*. https://doi.org/10.1108/jpcc-01-2024-0016
24. Saglam, R. B., Miller, V., & Franqueira, V. (2023). A Systematic Literature Review on Cyber Security Education for Children. *IEEE Transactions on Education*, 66, 274-286. https://doi.org/10.1109/te.2022.3231019
25. Saquib, N., Saquib, J., Wahid, A., Ahmed, A. A., Dhuhayr, H. E., Zaghloul, M. S., Ewid, M., & Al-Mazrou, A. (2017). Video game addiction and psychological distress among expatriate adolescents in Saudi Arabia. *Addictive Behaviors Reports*, 6, 112 - 117. https://doi.org/10.1016/j.abrep.2017.09.003
26. Sharma, A., & Mittal, S. (2021). Cyberbullying among Indian adolescents: Prevalence, forms and impacts. *Indian Journal of Psychological Medicine*.
27. Uramova, J., Segec, P., & Moravcik, M. (2024). Contribution to Safer Internet for Children at School. *2024 International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 1-7. https://doi.org/10.1109/iceta63795.2024.10850849
28. World Health Organization. (2020). *Protecting children from online harm: WHO technical note*. WHO.
29. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures. *Frontiers in Public Health*, 9. https://doi.org/10.3389/fpubh.2021.634909