



NATIONAL SAFETY COUNCIL OF INDIA

School Safety Awareness Campaign

Digital and Cyber Safety in Schools



Why this matters

A child's safety no longer ends at the school gate. Virtual classrooms, school WhatsApp groups, edtech platforms, and students' own devices have extended the school's duty of care into digital space. India's National Commission for Protection of Child Rights (NCPCR) treats cyber safety as a core dimension of school safety — not a specialist IT concern — and has been explicit that the safety of children in the digital space is the responsibility of the school or institution conducting the activity, online or offline.

The risks are well documented: cyberbullying and online harassment, grooming and sextortion, exposure to inappropriate content, non-consensual sharing of images, and misuse of personal data collected through apps and online classes. The Information Technology Act, 2000, POCSO Act, 2012, and the Digital Personal Data Protection (DPDP) Act, 2023 each impose specific, binding obligations relevant to how schools and edtech platforms must handle children online.



Core Digital and Cyber Safety Requirements

The following requirements consolidate NCPCR's cyber safety and anti-bullying guidance with the statutory obligations schools carry once they use digital tools, platforms, or online classes with children.

1. A Documented Cyber Safety and Acceptable Use Policy

Schools should maintain a written policy covering acceptable use of school devices, networks, and platforms; rules for student conduct online; and the school's response procedure for cyberbullying, harassment, or exposure to harmful content. NCPCR's guidance frames cyber safety as being about more than blocking technology — it requires staff and students to be digitally literate and to understand the etiquette, risks, and legal consequences of online behaviour, not just technical restrictions.

2. Controlled, Teacher-Supervised Virtual Classrooms

Following NCPCR's 2020 advisory on online classes, schools must ensure entire control of the virtual classroom rests with the teacher, with students joining only as guests rather than through accounts that expose personal login credentials. Login IDs should not be created in a student's own name where this is avoidable, and schools should vet and approve any app or platform used for children before it is adopted, rather than leaving this choice to individual teachers or vendors.

3. Parental Orientation and Supervision

NCPCR's guidance specifically calls for schools to provide proper orientation to parents so that a child's participation in virtual classrooms happens under parental supervision. This is not a one-time notice; schools should periodically remind parents what platforms are in use, what data those platforms collect, and how to report a concern, consistent with the shared responsibility model NCPCR promotes between schools and families.

4. An Anti-Bullying and Anti-Cyberbullying Committee

In line with NCPCR's 2024 Guidelines for Schools on Preventing Bullying and Cyberbullying, every school should establish a designated committee responsible for preventing, receiving reports of, and responding to bullying in both physical and online spaces. The guidelines recognise that cyberbullying can occur through text messages, apps, social media, gaming, and edtech or online learning platforms, and that new platforms will keep emerging — so the committee's mandate should be defined by the behaviour, not a fixed list of platforms.

5. Staff Digital Literacy and Training

Schools must ensure staff are digitally literate enough to teach students about digital etiquette, recognise signs of online distress or cyberbullying, and respond appropriately rather than dismissing online incidents as outside the school's concern. NCPCR's guidelines call for regular training and awareness programmes for both students and teachers covering online risks, gender sensitisation, and the psychological and legal consequences of bullying online.

6. Lawful Handling of Children's Personal Data

Section 9 of the Digital Personal Data Protection (DPDP) Act, 2023 treats anyone under 18 as a child for data protection purposes and requires verifiable parental or guardian consent before a child's personal data is processed. Schools and the edtech platforms they adopt should be able to show what student data is collected, why, and how consent was obtained — this is a compliance obligation for the institution, not solely the platform vendor's responsibility.

7. A Clear, Child-Friendly Reporting Pathway

Students need to know, in plain terms, how to report online harassment, grooming attempts, or inappropriate content — to a specific named teacher or counsellor, not an abstract policy. NCPCR's cyber safety guidance specifically advises children never to switch on a webcam for an unknown person and never to meet anyone they have only interacted with online without an adult present; schools should reinforce this messaging directly with students, not only with parents.

Recognising and Responding to an Incident

NCPCR's guidance sets out concrete first steps for both adults and children when a cyber safety concern arises. Schools should ensure these steps are known and rehearsed, not buried in a policy document no one has read.



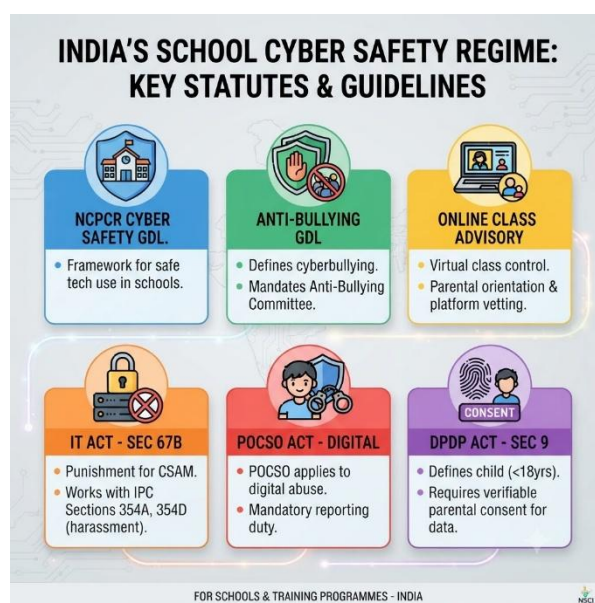
If a Child Reports a Concern	School's Immediate Response
• Inform a parent, elder, or teacher immediately rather than handling it alone • Block the person involved without engaging further • Save and preserve messages or screenshots as evidence • Avoid deleting the evidence even if it feels easier to do so	• Take the report seriously regardless of which platform was involved • Involve the designated anti-bullying/cyberbullying committee promptly • Escalate to parents and, where the conduct may be a criminal offence, to the police or Special Juvenile Police Unit • Document the response and follow up with the affected student

The accountability principle

NCPCR has stated plainly that neglecting the safety and security of children in the digital space, in any manner, can attract strict action against the school or institution under Section 75 of the Juvenile Justice (Care and Protection of Children) Act, 2015, alongside other relevant provisions of law. A school that adopts an edtech platform without vetting it, or that fails to act on a reported cyberbullying incident, carries the same institutional exposure online as it would for a physical safety lapse on campus.

Resources for Schools and Training Programmes

The following statutes, guidelines, and reporting mechanisms underpin India's school cyber safety regime and can inform NSCI's training content, institutional audits, and member-organisation advisories.



Statutes, Guidelines, and Statutory Bodies

- **NCPCR Guidelines on Cyber Safety:** Sets out the framework for safe and responsible use of information and communication technology in schools, covering staff and student awareness, risk categories, and specific child-facing advice such as never sharing a webcam feed with an unknown person.
- **NCPCR Guidelines for Schools on Preventing Bullying and Cyberbullying, 2024:** Defines bullying and cyberbullying, applies to all schools and educational institutions across India, and sets out the institutional structures — including a dedicated anti-bullying/cyberbullying committee — schools must put in place.
- **NCPCR Advisory on Safety of Children in Online Classes, 2020:** Issued during the COVID-19 lockdown, this advisory remains the clearest statement of NCPCR's expectations for virtual classroom control, parental orientation, and platform vetting, and explicitly ties non-compliance to liability under the Juvenile Justice Act.
- **Information Technology Act, 2000 — Section 67B:** Provides stringent punishment for publishing, browsing, or transmitting child sexual abuse material in electronic form, and works alongside Sections 354A and 354D of the Indian Penal Code addressing online harassment and stalking.
- **Protection of Children from Sexual Offences (POCSO) Act, 2012:** Applies fully to digital sexual exploitation and abuse of children, including grooming and the use of digital platforms to facilitate offences, with the same mandatory reporting duty under Section 19 that applies to offline conduct.
- **Digital Personal Data Protection (DPDP) Act, 2023 — Section 9:** Defines a child as any person below 18 years for data protection purposes and mandates verifiable parental or guardian consent before processing a child's personal data, directly relevant to school use of apps and edtech platforms.

Reporting Channels and Helplines

These channels should be displayed alongside other school safety information and included in induction and digital-citizenship material for staff, students, and parents.

Channel	Contact
Childline (24-hour, for children in distress)	1098
National Cyber Crime Reporting Portal	cybercrime.gov.in
Cyber Crime Helpline	1930
NCPCR POCSO e-Box (online sexual offences)	ncpcr.gov.in / POCSO e-Box
Police / Special Juvenile Police Unit	100 / 112

Verification and Audit Checklist

Drawing directly from NCPCR's cyber safety and online-classes guidance, NSCI recommends institutions confirm the following during every safety audit:

- Written cyber safety / acceptable use policy current and communicated to staff, students, and parents
- All online classes and platforms teacher-controlled, with students joining as guests where possible
- Apps and edtech platforms vetted and approved by the school before use with children
- Anti-bullying and cyberbullying committee designated, active, and known to students
- Staff trained periodically on digital literacy, online risks, and reporting procedures
- Parental orientation on digital safety conducted and refreshed periodically
- Data collected by school-used platforms documented, with parental consent obtained where required
- Clear, named reporting pathway known to students for cyberbullying, grooming, or inappropriate content

Share this article. One message Can help build safe digital world for kids

IS YOUR SCHOOL READY TO LEAD BY EXAMPLE?

Participate in the NSCI School Safety Awards and showcase your commitment to creating a safer school for every child.



National Safety Council of India

Website : <https://nsc.org.in/school-safety.aspx>

LinkedIn: [linkedin.com/company/nscindia](https://www.linkedin.com/company/nscindia)

Write to us : safetyaward@nsc.org.in

NATIONAL SAFETY COUNCIL OF INDIA

NSCI SAFETY AWARDS FOR SCHOOL

RECOGNIZING EXCELLENCE IN SCHOOL SAFETY
NSCI SAFETY AWARD

AWARD YEAR 2026

Objective:
To recognize and reward the school for promoting exemplary commitment to promoting safety awareness among the students and maintaining a safe, secure, and supportive school environment for all students and staff.

SAFE SCHOOL BRIGHT FUTURE

CELEBRATING SAFETY. HONORING EXCELLENCE.

STUDENT TRAINING
SAFETY FIRST

FIRE TRAINING

LABORATORY

FIRST AID

AWARENESS
Building Awareness, Saving Lives

PREPAREDNESS
Prepare Today, Stay Safe Tomorrow

SAFE TRANSPORT
Safe Rides, Bright Futures

SECURITY
Secure Campus, Secure Future

WELL-BEING
Healthy Minds, Happy Lives

RESPONSIBILITY
Responsible Today, Reliable Always

ENCOURAGING EXCELLENCE ★ RECOGNIZING EFFORTS ★ BUILDING A SAFER TOMORROW

