STUDY NOTES · BASIC CONCEPT

What are the major online risks faced by children?

Society & Social Justice

17 Oct 2026

Children can encounter several forms of online harm, and different risks require different responses.

Risk	Meaning	Suitable response
Cyberbullying	Harassment, humiliation or intimidation through digital platforms	Reporting tools, moderation, school support and appropriate enforcement
Online grooming	Building trust with a child to facilitate exploitation or abuse	Detection of predatory behaviour, reporting mechanisms and law enforcement
Child sexual exploitation and abuse material (CSEAM)	Material depicting or documenting sexual exploitation or abuse of children	Rapid detection and removal, preservation of evidence and investigation
Doxxing and privacy violations	Disclosure or misuse of personal information	Privacy-by-default settings, data minimisation and effective remedies
Sexual extortion	Threatening a person to obtain money, images or other benefits	Safe reporting channels, victim support and investigation
Harmful recommendation systems	Algorithms that may repeatedly expose users to damaging or age-inappropriate material	Safer design, content controls and accountability
Excessive or compulsive use	Patterns of use that disrupt sleep, education or wellbeing	Digital literacy, healthy-use guidance and age-appropriate design

BECOME IAS
AI-Powered UPSC Preparation by ENKI OT

The policy objective should be to reduce the probability and severity of these harms without unnecessarily depriving children of legitimate digital opportunities.

Important laws and institutions relevant to online child safety in India

A. Protection of Children from Sexual Offences (POCSO) Act, 2012 : The POCSO Act establishes a legal framework to protect children from sexual offences and provides for child-sensitive procedures.

Its relevance to online safety includes offences involving sexual exploitation and abuse, including circumstances in which digital platforms are used to contact, threaten or exploit children. Specific criminal liability depends on the conduct and applicable statutory provisions.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

B. Information Technology Act, 2000 : The IT Act provides a legal framework for electronic records, cyber offences and intermediary-related matters.

Section 67B addresses specified forms of publishing, transmitting and facilitating material depicting children in sexually explicit acts, as defined by the provision. Section 79 provides a conditional safe-harbour framework for intermediaries, subject to statutory requirements.

C. Information Technology Rules, 2021 : The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, establish due-diligence obligations for covered intermediaries and grievance-related mechanisms.

The precise obligations vary by the type of intermediary and the applicable provisions. The rules should not be interpreted as imposing an identical duty on every digital service.

D. Digital Personal Data Protection Act, 2023 : The Act establishes a framework for the processing of digital personal data, including specific provisions relating to children's data. Its provisions include parental-consent requirements for processing children's personal data, subject to the statutory framework and applicable rules, exemptions and implementation arrangements.

This is relevant to age verification, parental consent and the collection of identity information. A child-protection system must avoid creating unnecessary privacy risks while attempting to verify age.

E. National Commission for Protection of Child Rights (NCPCR) : The NCPCR is a statutory body established under the Commission for Protection of Child Rights Act, 2005. It monitors safeguards for children's rights and can play a role in addressing systemic child-protection concerns.

F. Ministry of Electronics and Information Technology (MeitY) : MeitY is central to digital-policy and intermediary-regulation matters. In the present proceedings, the Court considered measures to improve the prevention, reporting and removal of CSEAM from online platforms.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

What is CSEAM, and why is it central to the case?

CSEAM stands for Child Sexual Exploitation and Abuse Material. It refers to material associated with the sexual exploitation or abuse of children.

The issue is not merely that such material may be available online. It can be reproduced, redistributed and made accessible across platforms, creating repeated harm to victims and complicating enforcement.

An effective response requires a coordinated system involving:

1. Prevention of the creation and distribution of abusive material.
2. Detection and prompt removal of illegal content.
3. Reporting mechanisms accessible to children and caregivers.
4. Cooperation among platforms, regulators and law-enforcement agencies.
5. Preservation of relevant evidence in accordance with law.
6. Support for victims and protection of their identity and dignity.
7. Accountability for individuals and entities that violate applicable laws.

The Supreme Court's proceedings concern improving these mechanisms. Its discussion of internet access makes the broader point that restricting victims' access is not a substitute for preventing abuse and holding perpetrators accountable.

Age verification and the right to privacy

Age verification is often proposed as a way to restrict children's access to particular platforms or content. However, verifying age can create its own privacy challenges.

A system that requires every user to upload identity documents could expose personal information, create databases vulnerable to misuse, or enable unnecessary tracking. A poorly designed system may also exclude adults who lack particular documents or children who have legitimate reasons to access educational services.

Approach	Potential benefit	Potential risk
Uploading government identity documents	Can provide strong evidence of age in some circumstances	Collects sensitive identity information and may create security risks
Parental consent	Involves caregivers in decisions about younger users	Can be difficult to verify reliably and may exclude children without available parental support
Privacy-preserving age assurance	May confirm an age threshold without revealing full identity	Technical limitations, implementation costs and risks of error
Child-mode settings	Can limit unwanted contact, exposure and advertising	May be bypassed or provide incomplete protection

The policy principle is to collect the minimum information necessary, limit its retention and use, secure it appropriately and provide accessible alternatives where possible.

The Court's concern about age verification is not that age-based safeguards are always impermissible. It is that safeguards should be effective and proportionate, without imposing unnecessary surveillance on the entire population of internet users.

Digital divide: why internet access matters for equality

The digital divide is the gap between individuals or communities in their ability to access and effectively use digital technologies.

It includes more than the absence of an internet connection. It also involves differences in device availability, affordability, connectivity quality, digital literacy, language access and accessibility for persons with disabilities.

The digital divide can reinforce existing inequalities:

1. Rural students may depend on online resources where local educational facilities are limited.
2. Low-income families may have fewer devices and less reliable connectivity.
3. Children with disabilities may depend on accessible digital services.
4. Girls and other disadvantaged children may face unequal access to devices and digital autonomy.
5. Children who lack digital literacy may be more vulnerable to scams, misinformation and exploitation.

A blanket ban could affect children differently depending on their circumstances. A child with several offline educational resources may be less affected than a child whose schoolwork, assistive technology or communication depends heavily on internet access.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

Thus, child protection should be designed alongside digital inclusion.

What are the arguments for and against age-based social-media restrictions?

The debate should not be reduced to a choice between unrestricted social media and a complete ban on internet access.

Arguments supporting restrictions	Concerns about broad restrictions
Children may face grooming, cyberbullying and sexual exploitation	Restrictions may also block educational and supportive uses

Arguments supporting restrictions	Concerns about broad restrictions
Younger users may struggle to assess risks independently	Children may migrate to less-regulated services
Recommendation systems can expose children to unsuitable material	Age verification may compromise privacy
Parental controls alone may be inadequate	Enforcement may be uneven and easy to circumvent
Some services use engagement designs that encourage excessive use	Blanket bans can burden children instead of addressing platform design and offender behaviour

A sound policy should distinguish between access to the internet, access to particular social-media services and access to specific harmful content. Different risks may justify different safeguards.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

What are the major implementation challenges?

1. First, enforcement across platforms: Harmful content can move between services and jurisdictions. Cooperation among platforms, regulators and law-enforcement agencies is essential.
2. Second, privacy and age assurance: Authorities must determine how to verify age or parental consent without creating unnecessary identity databases or surveillance.
3. Third, unequal digital access: Safeguards should not inadvertently exclude disadvantaged children from education, assistive technologies or essential public services.
4. Fourth, platform incentives: Services may have commercial incentives to maximise engagement. Regulation must address design and recommendation practices where they contribute to harm.
5. Fifth, child-friendly reporting: Children need confidential, accessible reporting systems and assurance that seeking help will not automatically result in punishment.
6. Sixth, institutional capacity: Schools, parents, police, child-protection bodies and digital regulators require training, resources and clear responsibilities.

Important Supreme Court cases for UPSC

Case	Year	Significance
Anuradha Bhasin v. Union of India	2020	Recognised constitutional protection for speech and trade exercised through the internet and emphasised proportionality and safeguards in internet restrictions
Justice K. S. Puttaswamy (Retd.) v. Union of India	2017	Recognised privacy as a fundamental right under the Constitution, subject to applicable constitutional limitations
Pragya Prasun v. Union of India	2025	Recognised the importance of digital access in the context of accessibility and the rights of persons with disabilities
Just Rights for Children Alliance v. S. Harish	2026	In the October 15, 2026 order, recognised internet access and use as a fundamental right under Articles 21 and 19(1)(a), including for children, while addressing online child sexual exploitation and abuse material

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

The present ruling builds on the constitutional relationship between internet-based expression, personal liberty, privacy and access to digital services.

Prelims facts to remember

-

1. Article 19(1)(a): Freedom of speech and expression.
2. Article 19(2): Permissible reasonable restrictions on that freedom.
3. Article 21: Protection of life and personal liberty.
4. Article 21A: Free and compulsory education for children aged 6–14.
5. Article 14: Equality before the law and equal protection of laws.
6. POCSO Act, 2012: Protection of children from sexual offences.
7. Information Technology Act, 2000: Includes provisions relevant to cyber offences and child sexual abuse material.
8. IT Rules, 2021: Intermediary due diligence and related regulatory framework.
9. Digital Personal Data Protection Act, 2023: Includes provisions concerning children's personal data.
10. Doctrine of proportionality: A restriction on rights must be justified and proportionate to its legitimate objective.

11. Digital divide: Unequal access to and ability to use digital technologies.
12. CSEAM: Child Sexual Exploitation and Abuse Material.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT