

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 708
TO BE ANSWERED ON: 24.07.2026

REGULATION OF SOCIAL MEDIA FOR CHILDREN AND ADOLESCENTS

708. MS. SWATI MALIWAL:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

- (a) the steps taken by Government to assess the psychological and behavioural impact of excessive social media use on children and adolescents in the country;
- (b) whether any age-verification or parental consent mechanisms have been mandated for social media platforms;
- (c) the number of complaints received regarding harmful content targeting minors on social media platforms during the last three years, State-wise; and
- (d) whether Government proposes to introduce specific safeguards, such as age restricted usage, screen-time alerts or algorithmic transparency requirements, to protect children from addictive design features on these platforms?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): The Government is committed to ensuring an open, safe, trusted and accountable Internet for all users, particularly children. As Internet usage and digital access have expanded rapidly, children's exposure to inappropriate content and other online risks has also increased.

In order to protect the children and adolescents from the harmful effects of social media, Government has adopted a series of measures for preventing the flow of such information.

Legal structure:

The Information Technology Act, 2000 ("IT Act") and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules"), together, have established a framework to promote digital well-being, user safeguards and responsible digital participation.

IT Act and IT Rules 2021:

The IT Act provides punishment for various cyber offences such as identity theft (section 66C), impersonation (section 66D), privacy violations (section 66E), publishing or transmitting obscene or sexually explicit content (sections 67, 67A, 67B). It also empowers Police to investigate offences (Section 78 and 80).

With regard to inappropriate and unlawful content on the Internet, IT Act and the IT Rules, 2021, together, have put a stringent framework to deal with unlawful content in the digital space. Importantly, the guidelines explicitly cover child sexual exploitation material, non-

consensual intimate imagery, impersonation and other harmful AI-generated content, requiring platforms to prevent such content and take prompt action when detected.

IT Rules 2021 mandates the Significant Social Media Intermediaries (SSMIs) to take reasonable efforts to deploy appropriate technical measures, including automated tools or other suitable mechanisms, to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed.

Further, IT rules 2021 has been amended for strengthening of timelines for compliance, including reduced timelines for removal of unlawful information upon actual knowledge upon valid reasoned intimation from the Appropriate Government or court orders (timeline reduced from 36 hours to 3 hours) and for grievance redressal (including special categories such as nudity/impersonation etc.) (timeline reduced from 72 hours to 36 hours and 24 hours to 2 hours for sensitive matters, respectively).

Obligations of intermediaries:

The IT Rules require that the intermediaries shall observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful to children or violates any law for the time being in force.

Intermediaries, in cases where the violation involves the commission of an offence under any law currently in force—such as the Bharatiya Nyaya Sanhita, 2023 read with the Bharatiya Nagarik Suraksha Sanhita, 2023, or the Protection of Children from Sexual Offences Act, 2012, which mandates reporting must report such offence to the appropriate authority in accordance with the provisions of the applicable law.

Data Protection:

Additionally, the Digital Personal Data Protection Act, 2023 (“DPDP Act”) has been enacted which establishes the legal framework to regulate the processing of digital personal data. The DPDP Act provides a legal framework for safeguarding children’s privacy online.

It mandates parental consent for processing children’s personal data and prohibits practices detrimental to their well-being such as tracking, behavioural monitoring or targeted advertising towards children.

Promotion and Regulation of Online Gaming (PROG) Act, 2025

PROG Act was enacted by Parliament in August 2025. It safeguards citizens especially children, from the growing menace of online money games. The Act prohibits online money gaming in view of its adverse social and financial consequences, including the risk of addiction among children and young persons.

Advisories and Standard Operating Procedure (SOP):

The government has issued multiple advisories to the intermediaries, including the Social Media Intermediaries, emphasizing the observance of due diligence obligations under the IT Act and IT Rules. The details of the advisories issued and SOPs formulated are as follows:

- Vide Advisory dated 29.12.2025, government reiterated to the intermediaries regarding observance of statutory due diligence obligations under the IT Act and IT Rules, for

preventing hosting, publication, transmission, sharing or uploading of vulgar, indecent, obscene, pornographic and other unlawful content on their platforms. It also advised the intermediaries to undertake an immediate review of their internal compliance frameworks, content moderation practices and user enforcement mechanisms, and to ensure strict and continuous adherence to the provisions of the IT Act and the IT Rules.

- An advisory dated 16.03.2026 was issued to intermediaries with respect to the generation, hosting, publication, transmission, sharing or uploading of abusive, defamatory, objectionable, derogatory and misleading synthetically generated information.
- A Standard Operating Procedure (“SoP”) to curtail dissemination of Non-Consensual Intimate Imagery (NCII) content on online platforms has been formulated and released on 11.11.2025. The SoP provides detailed guidance for victims, intermediaries and law enforcement agencies to ensure prompt and uniform action against the online dissemination of NCII content including intimate or morphed images shared without consent.

Awareness campaigns:

Government is implementing a project on ‘Information Security Education and Awareness (ISEA)’ for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene & cyber security among the masses.

So far, 6,650 awareness workshops have been conducted across the country covering 11.37 lakh+ participants, including school/colleges students, teachers, law enforcement, government personnel, and general public.

Further, multilingual awareness material in the form of handbooks, short videos, posters, brochures, cartoon stories for children, etc. published and disseminated through print, electronic, social media and www.isea.gov.in & <https://staysafeonline.in/>.

CERT-In also regularly shares safety and security tips and awareness posters, info-graphics and videos on its official websites and social media handles and is aimed at sensitizing internet users on cyber security attacks and frauds including online safety measures for children.

The Ministry of Education issued the PRAGYATA Guidelines on Digital Education in July 2020, which provide a framework for safe and effective online learning, including promotion of students’ well-being and responsible use of social media and electronic devices.

CBSE has supplemented these efforts through guidelines on digital etiquette, cyber-security training for teachers, publication of the ‘Cyber Security Handbook’, and advisories to schools for establishing Cyber Clubs to promote cyber safety awareness.

NCERT has also incorporated cyber safety in its curriculum, including a chapter on “Societal Impacts” in Classes XI and XII, and CIET-NCERT has developed and disseminated resource materials on cyber safety.

The National Commission for Protection of Child Rights (“NCPCR”) has conducted a study on “Effects (Physical, Behavioural and Psycho-social) of using Mobile Phones and other

Devices with Internet Accessibility by Children” in 2021. The study report is available at https://ncpcr.gov.in/uploads/165650458362bc410794e02_effect1.PDF.

Additionally, NCPCR has prepared following guidelines on Cyber Safety and Protection of children:

1. Guideline and standard content for raising awareness among children, parents, educators and general public titled “Being Safe Online” is available at https://ncpcr.gov.in/public/uploads/16613370496305fdd946c31_being-safe-online.pdf.

2. Guidelines on Cyber Safety (for inclusion in) Manual on Safety and Security of Children in Schools which is available at:

https://ncpcr.gov.in/uploads/16613369326305fd6444e1b_cyber-safety-guidline.pdf.

3. Guidelines for Schools for prevention of bullying and cyber bullying” which is available at: https://ncpcr.gov.in/uploads/1714382687662f675fe278a_preventing-bullying-andcyberbullying-guidelines-for-schools-2024.pdf.

‘Police’ and ‘Public Order’ are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cybercrime through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs. The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”. The latest published report may be accessed on :<https://www.ncrb.gov.in>
