

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1725
TO BE ANSWERED ON: 29.07.2026

AGE BASED RESTRICTIONS FOR ACCESS TO SOCIAL MEDIA PLATFORMS

1725. SHRI BASTIPATI NAGARAJU:

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

- (a) whether the Government has taken note of concerns relating to social media addiction, cyberbullying, exposure to harmful content, online grooming, privacy violations and mental health risks among children and adolescents and if so, the details thereof;
- (b) whether the Government is considering prescribing a minimum age or introducing age based restrictions for access to social media platforms and if so, the details and timeline thereof;
- (c) whether the Government proposes to mandate age-verification mechanisms, parental consent, child safety settings and enhanced safeguards for the protection of children's personal data on social media platforms and if so, the details thereof; and
- (d) whether the Government has constituted or proposes to constitute an expert committee or undertake stakeholder consultations for framing a regulatory framework for the protection of minors on social media platforms and if so, the details thereof?

ANSWER

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

(a) to (d): The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users, including children. With the expansion of the Internet and more and more citizens including children, accessing the internet services, the risk of exposure to inappropriate content and the harmful effects of these activities have also increased. The Government is cognizant of the immense opportunities offered by these technologies and the harms they may cause. In order to protect the children and adolescents from exposure to inappropriate content and 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.

Information Technology Act , 2000 ("IT Act")

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).

Obligations of intermediaries under IT Act and IT Rules

The Government after extensive public consultations with relevant stakeholders has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule, 2021 (“IT Rules”) on 25.02.2021 which were subsequently amended from time-to-time to address emerging harms from misuse of technologies, including Artificial Intelligence (AI). 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.

Recent amendments

The Government regularly engages with relevant stakeholders to examine the legal, policy and institutional framework relating to emerging issues in the cyberspace, in light of technological developments and public interest. Any legislative or regulatory measures, if considered necessary, are processed in accordance with the extant policy and established legislative procedures of the Government.

On 10th February, 2026, the Government strengthened the regulatory framework by amending the IT Rules, 2021 to address harms arising from synthetically generated information (SGI), including deepfakes and AI-generated content.

Key points related to the amendment are as follows:-

- Intermediaries are required to ensure clear labelling and traceable metadata for permissible AI-generated content, so that users can easily identify synthetic cally generated material and prevent deception or misuse.
- It further strengthens user accountability and platform due diligence, including mandatory user awareness regarding legal consequences of unlawful AI-generated content and stronger compliance obligations for social media intermediaries.
- 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.
- 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).
- Intermediaries are obligated to deploy reasonable and appropriate technical measures, including automated tools or other suitable mechanisms, to not allow any user to create, generate, modify, alter, publish, transmit, share, or disseminate, as the case may be, any synthetically generated information that 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.

IT Rules 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.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, they lose their exemption from third party information provided under section 79 of the IT Act. They are liable for consequential action or prosecution as provided under any extant 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.

The Act expressly provides safeguards for children by requiring the Data Fiduciary to obtain verifiable parental consent before processing any personal data of a child. The Act also prohibits Data Fiduciary from tracking or behavioural monitoring of children or targeted advertising directed at children.

The DPDP Rules prescribe operational mechanisms for obtaining verifiable parental consent, including through identity and age verification measures and the use of virtual tokens.

Prohibiting online money gaming

The Promotion and Regulation of Online Gaming Act, 2025, represents a major step to address digital addiction and financial harm among youth.

Digital addiction

The Economic Survey 2025-26 mentions digital addiction as a serious public health challenge affecting India's children and youth, particularly those aged 15-29 who enjoy near-universal smartphone and internet access.

The Survey further highlights its profound impacts on cognitive development, academic performance, workplace productivity, social connectedness, and mental health, manifesting as anxiety, depression, sleep disorders, cyber bullying, and financial losses from compulsive gaming, social media, and online gambling.

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.
