

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *73
TO BE ANSWERED ON: 24.07.2026

ADULT CONTENT IN MOBILE APPLICATIONS MEANT FOR CHILDREN

***73. SMT. RAJATHI :**

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

- (a) whether Government noticed sexually explicit advertisements on mobile applications meant for children;
- (b) the specific measures taken by Government to instruct stakeholders including Google play store, Apple app store and App developers to prevent exposure of these explicit contents; and
- (c) the specific measures taken by Government to ensure removal of Child Sexual Abuse Material (CSAM)?

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

- (a) to (c): A Statement is laid on the Table of the House

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *73 FOR 24.07.2026 REGARDING “ADULT CONTENT IN MOBILE APPLICATIONS MEANT FOR CHILDREN”

(a) to (c): The policies of the Government are aimed at ensuring an open, safe and trusted and accountable internet for its users, including children.

The Information Technology Act, 2000 (“IT Act”) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, (“IT Rules”) together, have put in place a stringent framework to deal with unlawful and harmful content in the digital space.

CSAM material on social media and mobile applications meant for children:

Government of India took serious note of the recent reports of advertisements linked to child sexual abuse material CSAM on these platforms. Notices have been issued to these platforms to take immediate corrective measures.

National Commission for Protection of Child Rights (“NCPCR”) has also issued notices to these social media platforms.

Legal structure:

IT Act and the IT Rules, together, have established a framework to promote digital well-being, user safeguards and responsible digital participation.

Information Technology (IT) 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:

IT Rules require the intermediaries to observe due diligence while discharging their duties. They 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.

Significant social media intermediaries (i.e., social media intermediaries having 50 lakhs or above registered user base in India) are also required to ensure compliance to certain additional due diligence obligations:

- Appoint local officers (Chief Compliance Officers, Nodal Contact Persons, Resident Grievance Officers), and share physical address based in India for compliances and law enforcement coordination
- Publish monthly compliance reports
- 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

- SSIMs offering messaging services must help law enforcement trace originators of serious or sensitive content
- Offer voluntary user verification, internal appeals, and fair hearing before taking *suo-moto* action

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.

Recent amendments:

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 to ensure clear labelling and traceable metadata for permissible AI-generated content, so that users can easily identify synthetically 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.
- Reduced timeline for removal of unlawful information upon actual knowledge upon valid reasoned intimation from the Appropriate Government or court orders (reduced from 36 hours to 3 hours)
For grievance redressal (including special categories such as nudity/impersonation etc.) timeline was 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.

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.

Blocking harmful content:

The government has also disabled 50 OTT Platforms for public access in India in last two years for displaying obscene content and for violation of Section 67 and 67A of the IT Act, Section 294 of the BNS and Section 4 of the Indecent Representation of Women (Prohibition) Act, 1986.

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/college 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.
