GOVERNMENT OF INDIA
MINISTRY OF WOMEN AND CHILD DEVELOPMENT

RAJYA SABHA
UNSTARRED QUESTION NO. 2238
TO BE ANSWERED ON 11.03.2026

CYBER SAFETY AND ONLINE PROTECTION FOR WOMEN AND GIRLS

2238. SHRI SUJEET KUMAR:

Will the Minister of WOMEN AND CHILD DEVELOPMENT be pleased to state:

a. whether Government is taking specific measures to address cyber bulling, online stalking and harassment of women and girls;

b. if so, the nature of awareness campaigns, school outreach and digital literacy programmes being conducted; and

c. whether any partnership exists between the Ministry and technology platforms to monitor and report gender-based online abuse?

ANSWER

THE MINISTER OF WOMEN AND CHILD DEVELOPMENT
(SHRIMATI ANNPURNA DEVI)

(a) to (c): States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of crimes, including cyber-crimes, through their Law Enforcement Agencies (LEAs). The Central Government supports these efforts by issuing advisories and providing financial assistance under various schemes to enhance capacity building.

To strengthen a comprehensive and coordinated response mechanism to deal with cyber crimes, the Central Government has implemented measures such as raising public awareness, issuing alerts and advisories, training LEAs personnel, prosecutors, and judicial officers, and upgrading cyber forensic facilities. In this regard, the Indian Cyber Crime Coordination Centre (I4C) has been established as an attached office of the Ministry of Home Affairs to create a robust framework and ecosystem for LEAs.

A key component of I4C is the National Cyber Crime Reporting Portal (NCCRP) at https://cybercrime.gov.in, which enables the public to report all types of cyber crimes, with special emphasis on those against women and children. It offers dedicated facilities for reporting Child Sexual Exploitative and Abuse Material (CSEAM) and Rape/Gang Rape (RGR)-related content, including anonymous reporting and trackable complaint mechanisms. Reported incidents are processed by the States and UTs LEAs concerned, which handle FIR registration, chargesheet filing, arrests, and resolutions in accordance with legal provisions.

Under the Cyber Crime Prevention against Women and Children (CCPWC) Scheme, the Ministry of Home Affairs has released ₹132.93 crores in financial assistance to States and UTs for capacity building, including establishment of cyber forensic-cum-training laboratories, hiring of junior cyber consultants, and training of LEA personnel, public prosecutors, and

judicial officers. Consequently, 33 such laboratories have been commissioned across States and UTs, and over 24,600 LEA personnel, judicial officers, and prosecutors have received training in cybercrime awareness, investigation, and forensics.

On 26 April 2019, a Memorandum of Understanding (MoU) was signed between the National Crime Records Bureau (NCRB), India, and the National Centre for Missing and Exploited Children (NCMEC), USA, to facilitate sharing of Tipline reports on online child pornography and child sexual exploitation content with States and UTs concerned. Additionally, NCRB has been designated as a Government of India agency authorized to issue notices to intermediaries under Section 79(3)(b) of the Information Technology Act for removal of Child Pornography (CP) and Rape & Gang Rape (RGR) content.

The National Commission for Protection of Child Rights (NCPCR) has developed key resources to promote online safety. In 2017, it released "Being Safe Online," a guideline and standard content for awareness among children, parents, educators, and the public, available at https://ncpcr.gov.in/uploads/16613370496305fdd946c31_being-safe-online.pdf.

NCPCR also issued a Manual on Safety and Security of Children in Schools in 2017-18, updated in 2020-21 to incorporate guidelines preventing cyber bullying. This manual details cyber safety measures, including Do's and Don'ts for students, and steps for prevention and countermeasures, accessible at https://ncpcr.gov.in/uploads/165650391762bc3e6d27f93_manual-on-safety-and-security-of-children-inschools-sep-2021.pdf.

In 2024, NCPCR released guidelines on Preventing Cyber Bullying for school children, offering comprehensive information on cyber bullying, reporting mechanisms, prevention strategies in schools, homes, and cyberspace, along with Do's and Don'ts for teachers and management, and recommendations for educators and caregivers. These are available at https://ncpcr.gov.in/uploads/1714382687662f675fe278a_preventing-bullying-and-cyberbullyingguidelines-for-schools-2024.pdf.

During 2025-26, NCPCR conducted 38 conferences at State and district levels across India on child rights issues, including school safety (encompassing cyber safety) and the POCSO Act, engaging school stakeholders. It also organized a four-day virtual capacity-building programme in collaboration with the Atomic Energy Education Society (AEES) for school administrators and educators on child protection laws and safety practices. Further, NCPCR is conducting virtual district workshops on school safety and child security in March and April 2026.

The Information Technology Act, 2000 (IT Act) and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) collectively establish a comprehensive framework to address unlawful content in the digital space.

The IT Act penalizes the publishing or transmission of sexually explicit acts in electronic form (Sections 67A and 67B) and obscene material in electronic form (Section 67), with imprisonment extendable to five and three years, respectively. Relevant provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS 2023) further apply:

- Section 294 addresses offences related to the sale of obscene material, including its display in electronic form.
- Section 296 provides punishment for obscene acts and songs.

- Section 353 curbs misinformation and disinformation by penalizing false or misleading statements, rumours, or reports that may cause public mischief or fear.

The IT Rules impose specific obligations on intermediaries, including social media platforms, to ensure users do not host, display, upload, modify, publish, transmit, store, update, or share obscene, pornographic, paedophilic, child-harming, privacy-invasive, gender-insulting, or harassing content, or material violating any law. Intermediaries must expeditiously remove such unlawful content within stipulated timelines.

*****