GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 2952
TO BE ANSWERED ON: 06.08.2025

CYBER SAFETY OF CHILDREN

2952. DR. GUMMA THANUJA RANI:

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

(a) the number of children who were exposed to cyber threats during the last three years;
(b) whether the Government has taken any comprehensive steps to reduce exposure of children to cyber threats;
(c) if so, the details thereof and if not, the reasons therefor;
(d) whether the Government proposes to launch a cyber safety policy for children to address the emerging challenges; and
(e) if so, the details thereof and if not, the reasons therefor?

ANSWER

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

(a) to (e): The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The latest published report is available at https://www.ncrb.gov.in/crime-in-india.html

Government has taken various steps to reduce exposure of children to cyber threats:

Information Technology Act, 2000 ('IT Act') and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('IT Rules')

- Clear objective of online safety of users, particularly children
- Section 67B of the IT Act penalises electronic material depicting children in a sexually explicit, obscene, or indecent manner - Cognisable offence
- Includes inducing them into online sexual relationships, facilitating abuse, or recording such acts
- Punishable with imprisonment of up to 5 years & up to ₹10 lakh fine on first conviction, and up to 7 years imprisonment with the same fine on subsequent convictions
- Section 77A of the IT Act: For offences made compoundable under the Act (other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided), the court shall not compound the offence if it has been committed against a child below the age of 18 years.

Key provisions under IT Rules, 2021:

Provision	Details
Restricted information under Rule 3(1)(b)	Restricts information/content that, among other things, · is obscene, pornographic, invasive of privacy, or promotes hate or violence; · harms children; · misleads or deceives, including through deepfakes; · impersonates others, including via AI; · threatens national security or public order; · violates any applicable law.
User Awareness Obligations	Intermediaries must clearly inform users through terms of service and user agreements about the consequences of sharing unlawful content, including content removal, account suspension, or termination.
Accountability in Content Removal	Intermediaries must act expeditiously to remove unlawful content upon court orders, government notice, or user grievances, within prescribed timelines.
Grievance Redressal	· Intermediaries to appoint Grievance Officers · Mandates to resolve complaints through removal of unlawful content within 72 hours. · Content violating privacy, impersonating individuals, or showing nudity must be removed within 24 hours against any such complaint.
Grievance Appellate Committees (GACs) Mechanism	Users can appeal online at www.gac.gov.in if their complaints are not addressed by the intermediaries' Grievance Officers. GACs ensure accountability and transparency of content moderation decisions.

Additional Obligations of significant social media intermediaries (SSMIs) (i.e., social media intermediaries having 50 lakhs or above registered user base in India)	· SSMIs offering messaging services must help law enforcement trace originators of serious or sensitive content. · SSMIs to use automated tools to detect and limit spread of unlawful content. · SSMIs to publish compliance reports, appoint local officers, and share physical address based in India for compliances and law enforcement coordination. · SSMIs to offer voluntary user verification, internal appeals, and fair hearing before taking suo-moto action.

Digital Personal Data Protection Act, 2023 ("DPDP Act")

- Establishes the legal framework to regulate the processing of digital personal data.
- Allows Data Fiduciaries to process the personal data of children only with parental consent
- Does not permit processing of personal data which is detrimental to well-being of children or involves tracking, behavioural monitoring or targeted advertising

Information Security Education & Awareness ("ISEA") Programme

- To generate awareness among users while using internet
- Dedicated website has been created for information security awareness that generates and upgrades relevant awareness material on a regular basis
- It can be accessed at https://staysafeonline.in/

Indian Computer Emergency Response Team (CERT-In)

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

The Protection of Children Sexual Offences (POCSO) Act, 2012 was enacted to safeguard children from sexual offences and prevent such crimes against children. It provides punishment as per the gravity of offence.

National Commission for Protection of Child Rights (NCPCR), a statutory body under Ministry of Women and Child Development has prepared following guidelines on Cyber Safety and Protection of children:

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

- NCPCR has a dedicated/ transparent Online Complaint System https://ncpcr.gov.in/ebaalnidan/, to ensure timely/speedy redressal of complaints of various violations and deprivation of child rights

Ministry of Education has issued advisories for parents and teachers on 'Overcoming online gaming downsides' and 'Children's safe online gaming'.

Ministry of Home Affairs (MHA) has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrime in the country, in a coordinated and comprehensive manner.

'**National Cyber Crime Reporting Portal**' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber-crimes, with special focus on cyber-crimes against women and children.

Cyber-crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the LEAs of State/UT concerned, as per the provision of law.

****