Ministry of Electronics & IT

Legal safeguards in place to prevent potential harms that may arise from AI and related technologies

Posted On: 11 MAR 2026 3:55PM by PIB Delhi

India's AI strategy is based on Hon'ble Prime Minister's vision of democratizing technology. It aims to address India centric challenges, create opportunities and ultimately improve the lives of citizens.

At the same time, the Government is conscious of the potential harms that may arise from AI and related technologies.

Legal safeguards are in place to prevent harm towards children:

1. Information Technology (IT) Act, 2000

IT Act, 2000 and IT Rules require intermediaries (social media platforms) to prevent hosting or sharing content that is harmful to children including content that is sexually explicit or promotes violence.

Platforms must remove unlawful content within 3 hours (2 hours for non-consensual sexual/intimate content) of being notified by the government or court order.

Platforms are also obligated to report to appropriate authorities about the related offences under laws such as Bharatiya Nagarik Suraksha Sanhita, 2023, or the Protection of Children from Sexual Offences Act, 2012.

2. Protection of Children's Data (DPDP Act, 2023)

Digital Personal Data Protection Act, 2023 and Rules, 2025 cover personal data collected through technologies including AI-powered toys

Act provides special safeguards for processing of personal data of children by mandating the verifiable consent of the parent or lawful guardian before processing any personal data of a child

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

The act and rules made there under prohibit tracking, behavioural monitoring or targeted advertising directed at children.

3. CERT-In regularly shares safety, security tips, and awareness posters, infographics, and videos on its official websites and social media handles to sensitise internet users about online safety measures for children.

4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (SPDI Rules).

These rules require organisations to collect personal data only for stated purposes, obtain consent before sharing it, and publish privacy policies. Sensitive personal data must not be published and must not be further disclosed by third parties.

5. India AI Governance Guidelines

These Guidelines promote human-centric and responsible AI development. It recognize that children constitute a vulnerable group that may face risks from AI systems, and long term harm.

The Guidelines recommend risk assessment frameworks and monitoring of AI-related harms to help policymakers better understand real-world risks from AI systems and design appropriate governance responses.

6. Regulatory Framework for Toy Safety and Harmful Content

Toys in India must comply with Toy Quality Control Order and BIS standards, while harmful or explicit content involving children is regulated under the IT Act, IT Rules and POCSO Act.

7. Information Security Education and Awareness (ISEA)

Programmes have been conducted for generating human resources in Information Security and creating general awareness on various aspects of cyber hygiene and cyber security.

So far, 4,309 awareness workshops conducted across the country covering over 9.63 lakh participants, including school/colleges students, teachers, law enforcement, government personnel, and general public. 1,186 awareness workshops were conducted for school children and students covering 3.38 lakh participants.

1.13 lakhs school teachers, police personnel & volunteers have been trained as master trainers in 66 programs and around 15 crores estimated beneficiaries covered through indirect mode.

8.Studies conducted by the National Commission for Protection of Child Rights (NCPCR):

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:

- 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 are available at:https://ncpcr.gov.in/uploads/16613369326305fd6444e1b_cyber-safety-guidline.pdf
- Guidelines for Schools for prevention of bullying and cyber bullying” are available at:https://ncpcr.gov.in/uploads/1714382687662f675fe278a_preventing-bullyingandcyberbullying-guidelines-for-schools-2024.pdf

National Council of Educational Research and Training has also released a handbook on “Safe online learning in times of COVID-19”. The handbook is available athttps://ncert.nic.in/pdf/announcement/Safetolearn_English.pdf

9.Additional measures to strengthen the national response to cybercrimes:

To further strengthen the mechanism to deal with such cybercrimes in a coordinated manner, the Government has also taken several other measures, including the following:

- Ministry of Home Affairs (MHA) operates National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report all cybercrimes, with special focus on crimes against children
- Indian Cyber Crime Coordination Centre (I4C) has been established to ensure coordinated and comprehensive action against cybercrime, including child sexual exploitation
- Financial assistance is provided to States/UTs under the Cyber Crime Prevention against Women and Children Scheme for capacity building, including cyber forensic laboratories and training of police, prosecutors and judicial officers
- Government periodically blocks websites containing Child Sexual Abuse Material (CSAM) based on inputs from Interpol, routed through the Central Bureau of Investigation (CBI)
- Internet Service Providers have been directed to dynamically block CSAM websites using global databases such as the Internet Watch Foundation (UK) and Project Arachnid (Canada)
- ISPs have also been advised to promote parental control filters and block access to identified CSAM websites, including through international gateways
- Public awareness on cyber safety is promoted through initiatives such as @CyberDost, radio campaigns, and publication of handbooks for students and adolescents

MoU has been done between NCRB (MHA) and the National Center for Missing and Exploited Children (NCMEC), USA . This enables sharing of tipline reports on online child sexual exploitation, which are further disseminated to States/UTs through the national portal for prompt action.

This information was provided by the Union Minister for Electronics & Information Technology Shri Ashwini Vaishnaw in Lok Sabha today.

****

MSZ