



Comprehensive and coordinated institutional framework put in place to prevent, detect and combat online sexual abuse and exploitation of children

प्रविष्टि तिथि: 05 AUG 2026 4:13PM by PIB Delhi

The Ministry of Women and Child Development, the Ministry of Electronics and Information Technology (MeitY) and the Ministry of Home Affairs (MHA) have, within their respective statutory domains, put in place a comprehensive and coordinated institutional framework to prevent, detect and combat the online sexual abuse and exploitation of children. These policies of the Government are aimed at ensuring an open, safe, trusted, and accountable internet for its users, including women and children in the digital space.

The Protection of Children from Sexual Offences (POCSO) Act, 2012 provides for safeguarding children against sexual offences, including online sexual abuse. Section 12 prescribes punishment for sexual harassment of a child, as defined under Section 11, including through electronic or online means, such as making sexually coloured remarks, showing pornographic material, or repeatedly contacting a child with sexual intent. Section 13 criminalises the use of a child for pornographic purposes in any form of media, including electronic, printed, or broadcast media, for the purpose of sexual gratification. Section 14 prescribes punishment with imprisonment for a term not less than five years and fine for the first offence, while a second or subsequent conviction attracts imprisonment for a term not less than seven years along with fine. Further, Section 15 provides a graded punishment framework for storing or possessing pornographic material involving children, including failure to delete, destroy, or report such material, depending upon the nature and purpose of the offence.

The Bharatiya Nyaya Sanhita (BNS), 2023 further strengthens the legal framework to address offences of online child sexual abuse. Section 294 criminalises sale, distribution, public exhibition or circulation of obscene material, including in electronic form, while Section 295 specifically prohibits sale, distribution or exhibition of obscene material to children.

The Information Technology (IT) Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provide a comprehensive legal framework to address online sexual offences against children. The IT Act prescribes punishment for offences such as identity theft, impersonation, privacy violations, and publication or transmission of obscene or sexually explicit content, and also empowers law enforcement agencies to investigate such offences. The IT Rules, 2021 impose due diligence obligations on intermediaries to prevent hosting or sharing content that is harmful to children or otherwise unlawful. Further, under Rule 3(2)(b), intermediaries are required to remove or disable access, within two hours of receipt of a complaint, to content involving full or partial nudity, sexual acts, or AI-generated/morphed intimate images.

The Central Government has further strengthened the regulatory framework through amendments to the IT Rules, 2021 to address harms arising from synthetically generated information (SGI), including deepfakes and AI-generated content, requiring intermediaries to remove unlawful content within three hours of receipt of an order of a competent court or a reasoned intimation from the Appropriate Government or its authorised agency.

The 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/>.

The Indian Computer Emergency Response Team (CERT-In) regularly issues guidelines on AI-related threats, including deepfakes, and disseminates safety advisories, awareness posters, infographics, and videos through its official website and social media platforms to promote cyber safety, including online safety for children. Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate Significant Social Media Intermediaries (SSMIs) to make reasonable efforts to deploy appropriate technical measures, including automated tools, to proactively identify content depicting rape, child sexual abuse or exploitation, or content identical to material previously removed.

'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act. The platform enables timely reporting, coordinated action, and expeditious compliance by intermediaries with lawful requests relating to Child Sexual Exploitation and Abuse Material (CSEAM) and other unlawful online content.

The Ministry of Home Affairs (MHA) operates a National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable citizens to report complaints pertaining to all types of cybercrimes, with special focus on cybercrimes against children. The Ministry has also set up the Indian Cyber Crime Coordination (I4C) to deal with all types of cybercrimes, including cybercrime against children, in a coordinated and comprehensive manner.

Department of School Education & Literacy (DOSEL), Ministry of Education has developed Guidelines on School Safety and Security, for safety and security of children studying in Government, Government-aided and Private Schools, in line with the provisions contained in the National Education Policy, 2020. The guidelines are advisory in nature and have been circulated to all States & UTs/Autonomous Bodies of DoSEL and stakeholder Ministries on 01.10.2021. The guidelines further states that in case of occurrence of any untoward incidents e.g., physical or sexual violence, bullying, injury etc., the school management should report the matter to the authorities concerned and immediately take necessary action and also corrective measures so that the incident do not recur.

The National Commission for Protection of Child Rights (NCPCR), a statutory body under the Ministry of Women and Child Development, regularly coordinates with the Indian Cyber Crime Coordination Centre (I4C) and the Ministry of Electronics and Information Technology (MeitY) to address Online Child Sexual Abuse and Exploitation (OCSAE). The Commission also conducts awareness programmes on child rights, including school safety, cyber safety, and the POCSO Act, at the State, district, and virtual levels. Further,

NCPCR has developed and periodically updated guidance documents, including *Being Safe Online* (2017), the *Manual on Safety and Security of Children in Schools* (updated in 2020–21), and the *Guidelines on Preventing Cyber Bullying for School Children* (2024), to promote digital safety, prevent cyber bullying, and enhance awareness among children, parents, teachers, and other stakeholders.

This information was given by the Minister of State for Women and Child Development Smt. Savitri Thakur in Rajya Sabha in reply to a question.

SS

(रिलीज़ आईडी: 2294855) आगंतुक पटल : 505
इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , हिन्दी , Tamil