Ministry of Electronics & IT

Government's measures to ensure safe and accountable internet

Posted On: 10 DEC 2025 3:26PM by PIB Delhi

The policies of the Government are aimed at ensuring an Open, Safe and Trusted and Accountable Internet for its users, including children.

With the expansion of the Internet and more users accessing it, the risk of exposure to inappropriate content and the harmful effects of these activities have also increased.

The Government is cognizant of this challenge and the harms arising out of exposure to content which is harmful, addictive, or age-inappropriate. The Government has adopted a series of measures to enhance platform accountability on social media.

Legal frameworks to counter unlawful content on social media platforms

Information Technology (IT) Act, 2000

The IT Act and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), together, have put in place a stringent framework to deal with unlawful and harmful content in the digital space and impose clear obligations on intermediaries to ensure accountability.

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), enter public place and search and arrest suspected person (section 80).

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The IT Rules, 2021 cast due-diligence obligations on intermediaries, including social media intermediaries, and require them to implement these obligations effectively so as to prevent the hosting or transmission of unlawful content.

Key provisions under IT Rules, 2021:

Provision	Details

Restricted information under Rule 3(1)(b)	Restricts hosting, storing, transmitting, displaying or publishing information/content that, among other things, is: • obscene, pornographic, invasive of another's privacy, insulting or harassing on the basis of gender, racially or ethnically objectionable, or promoting hate or violence; • harmful to child; • deceives or misleads, including through deepfakes; • impersonates others, including via Artificial Intelligence; • 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, reasoned intimation from Government, 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.
Assistance by Intermediaries to Government Agencies	Intermediaries must provide information under their control or assistance to authorised Government agencies for identity verification, or for the prevention, detection, investigation, or prosecution of offences, including cyber security incidents.

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.

In case of failure of the intermediaries to observe the legal obligations as provided in the IT Rules, 2021, 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.

Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act establishes the legal framework to regulate the processing of digital personal data of users. It allows Data Fiduciaries to process the personal data of children only with verifiable parental consent.

It also prohibits processing of personal data which is detrimental to the well-being of children or involves tracking, behavioural monitoring or targeted advertising.

Bharatiya Nyaya Sanhita (BNS), 2023

The BNS, 2023 strengthens the legal framework to address offences involving online harm, obscenity, misinformation and other cyber-enabled crimes, including those committed through social media platforms.

- Provides punishment for offences like obscene acts and songs (Section 296), sale of obscene material including display of any such content in electronic form (Section 294)
- Section 353 aims to curb the spread of misinformation and disinformation by penalizing the act of making false or misleading statements, rumours, or reports that can cause public mischief or fear.

Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO act defines a child as any person below the age of 18 years and provides for provisions to safeguard children against sexual abuse and sexual harassment.

- Section 13 criminalises the use of a child in any form of media—whether electronic, printed, or broadcast—for the purpose of sexual gratification.
- Section 14 prescribes punishment of imprisonment for not less than five years and a fine for the first offence. For subsequent convictions, the punishment increases to imprisonment for not less than seven years and a fine.

- Section 15 lays out a graded punishment system for possessing, storing, or failing to report pornographic material involving children.

Additional framework for protecting children

- National Commission for Protection of Child Rights has issued several guidelines to enhance cyber safety and create awareness among children, parents and schools. These include:

  i. Guideline and standard content for raising awareness among children, parents, educators and general public titled “Being Safe Online” which is available at

  https://ncpcr.gov.in/public/uploads/16613370496305fdd946c31_being-safe-online.pdf

  ii. 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

  iii. 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

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

India’s multi-layered cyber response ecosystem includes institutional, regulatory and public awareness mechanisms to address cyber crimes, user grievances, and unlawful content:

- **GACs**– Provide an appellate forum appeal against the decisions of intermediaries.
- **Indian Cyber Crime Coordination Centre (I4C)** – Coordinates actions related to cyber crimes across States.
- **SAHYOG Portal**– Enables automated, centralized intimations to intermediaries for removal of unlawful content by authorised agencies across India.
- **National Cyber Crime Reporting Portal** – Citizens can report incidents through this portal at https://cybercrime.gov.in (helpline number 1930) which has special focus on cyber crimes against women and children.
- **CERT-In** – The Indian Computer Emergency Response Team (CERT-In) regularly issues guidelines on cyber security threats and countermeasures.
- **Awareness campaigns** – MeitY observes the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 2nd Tuesday of February every year, Swachhta Pakhwada from 1st to 15th February of every year and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month by organising various events and activities for citizens as well as the technical cyber community in India.
- **Information Security Education & Awareness (“ISEA”)** program has been launched to generate awareness among users while using internet. A dedicated website has been created for information security awareness that generates and upgrades relevant awareness material on a regular basis and can be accessed at https://www.infosecawareness.in.

This information was submitted by Union Minister of State for Electronics and Information Technology Shri Jitin Prasada in Lok Sabha on 10.12.2025.

***

MSZ