Ministry of Electronics & IT

MeitY Issues Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content

SOP to Ensure Swift and Uniform Action Against NCII Content; Mandates Takedown Within 24 Hours of Reporting

New SoP Empowers Individuals to Reclaim Control Over Digital Identities; Reinforces Government's Commitment to Privacy, Dignity and Safety in Cyberspace

Posted On: 11 NOV 2025 5:55PM by PIB Delhi

The Ministry of Electronics and Information Technology (MeitY) has released a Standard Operating Procedure (SoP) to strengthen mechanisms for the removal and prevention of Non-Consensual Intimate Imagery (NCII) content on online platforms.

This initiative, developed in compliance with the directions of the Madras High Court (Writ Petition - Civil No.25017/2025, Order dated 15.07.2025), aims to provide clear and victim-centric procedures for swift removal of such objectionable content and to ensure effective implementation of Rule 3(2) (b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Purpose and Scope

The SoP provides detailed guidance for victims, intermediaries, and law enforcement agencies to ensure prompt and uniform action against the online dissemination of NCII content — including intimate or morphed images shared without consent. It lays out mechanisms for content takedown within 24 hours of reporting.

Key Features of the Standard Operating Procedure (SoP)

1. Multiple Reporting Avenues for Victims

- One Stop Centres (OSCs): Victims can approach the nearest OSC for assistance, including help with reporting through the National Cybercrime Reporting Portal (NCRP), legal support, and psychological counselling.
- Intermediaries: Victims may directly report content through in-app reporting mechanisms, grievance officers of the concerned intermediaries.

- National Cybercrime Reporting Portal (NCRP): Enables individuals to report incidents online or by dialling 1930.
- Law Enforcement Agencies (LEAs): Complaints can also be lodged at local police stations for immediate action.

2. Mandatory Timelines for Intermediaries

- All intermediaries are required to remove or disable access to flagged content within 24 hours of receiving a complaint.
- Significant Social Media Intermediaries (SSMIs) must use hash-matching and crawler technologies to prevent the reappearance of the same or similar content.
- Intermediaries must also report actions taken and ensure coordination with government portals like Sahyog under MHA - I4C (Indian Cybercrime Coordination Centre, Ministry of Home Affairs).

3. Inter-Agency Coordination

- Indian Cybercrime Coordination Centre, Ministry of Home Affairs: Acts as the central aggregator for NCII complaints and maintains a secure NCII hash bank.
- Department of Telecommunications (DoT): Coordinates with Internet Service Providers to block flagged URLs.
- MeitY: Monitors compliance and coordinates with intermediaries and other government stakeholders.

Empowering Victims and Strengthening Digital Safety

This SoP is a major step towards empowering individuals, especially women, to reclaim control over their digital identities and to ensure a safe online environment. It also reinforces the government's commitment to protecting privacy, dignity and safety in cyberspace.

The Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content is available at:

https://www.meity.gov.in/static/uploads/2025/11/a2c9500ef5f8b62a43bfc68747de592d.pdf

***

Dharmendra Tewari\Navin Sreejith