HANDBOOK & PLAYBOOK FOR LAW ENFORCEMENT AGENCIES

ONLINE CRIMES AGAINST WOMEN & CHILDREN

Legal Framework | Investigation | Prosecution

Covering IT Act 2000, BNS, BNSS, BSA, POCSO, DPDP Act & IT Rules 2026 | LEA Edition

OCWC Handbook | Law Enforcement Edition | 2026

Prepared by: Indian Cyber Crime Coordination Centre (I4C)

TABLE OF CONTENTS

Foreword, I4C History & Field Scope 3
Why this handbook matters for field officers 3
I4C, NCRP, NCPCR and partner bodies 3
Chapter 1 — Understanding Types of Online Crimes Against Women & Children 5
1.1 Cybercrimes Targeting Women 5
1.2 Cybercrimes Targeting Children 5
1.3 Emerging & Hybrid Crime Categories 6
Chapter 2 — Legal & International Framework 7
2.1 Indian Legislative Framework 7
2.2 Key BNS Provisions 7
2.3 POCSO Act, 2012 8
2.4 IT Act 2000 — Key Sections 8
2.5 IT Rules 2021 as amended in 2026 8
2.6 BSA & BNSS: Evidence and procedure 9
2.7 DPDP Act 2023 9
2.8 International Frameworks & Conventions 10
Chapter 3 — Investigation & Prosecution 11
3.1 FIR Registration — Procedure & Jurisdiction 11
3.2 Sections to be Invoked — Quick Reference 11
3.3 Steps for Evidence Collection 12
3.4 Digital Evidence Collection & Forensic Standards 13
3.5 Victim Statements & Victim Identification 13
3.6 Preparation of a Fool-Proof Chargesheet 14
3.7 NCRP, 1930, Sahyog and urgent takedown 14
3.8 Raid scene protocol without a cyber expert 15
3.9 Age determination, rehabilitation and monitoring 16
Chapter 4 — Important HC/SC Judgements & Key Takeaways 18
4.1 Supreme Court Landmark Judgements 18
4.2 High Court Notable Orders 19
4.3 Consolidated Key Takeaways 20
Annexures — Contact Portals, ISP Directory & Investigation Checklist 21

FOREWORD, I4C HISTORY & FIELD SCOPE

The proliferation of digital technologies has transformed everyday life, enabling communication and commerce at unprecedented scale. Yet these same platforms have opened new vectors of abuse — particularly against women and children, who remain disproportionately targeted in cyberspace. Online Crimes Against Women and Children (OCWC) encompass a vast spectrum of offences: from cyberstalking and non-consensual intimate image sharing to child sexual abuse material (CSEAM), online grooming, and sextortion.

This Handbook and Playbook has been authored as an operational reference for Law Enforcement Agencies (LEAs) — including police officers, cyber crime unit investigators, public prosecutors, judicial officers, and forensic professionals engaged in the investigation, prosecution, and prevention of OCWC. It consolidates, in a single accessible volume, the relevant Indian statutory provisions, international frameworks, step-by-step investigation protocols, and landmark judicial precedents.

> ***How to Use This Handbook:*** *Each chapter is self-contained and may be consulted independently by field officers. Chapter 1 provides conceptual grounding on offence typology; Chapter 2 consolidates all applicable law; Chapter 3 offers operational step-by-step guidance for LEAs; Chapter 4 distils judicial wisdom relevant to investigation and prosecution. Annexures provide quick-reference tables and field checklists.*

Why Field Officers Should Not Skip Legal Provision Checks

Wrong or incomplete charging is a recurring reason for delay, weak bail opposition, defective production orders and acquittal. A cyber sexual offence often needs multiple linked provisions: IT Act for electronic publication or transmission, BNS for harassment, stalking, extortion, trafficking or intimidation, POCSO for child victims, BNSS for procedural powers, and BSA Section 63 for admissibility of electronic records. The IO should record the factual basis for every invoked section in the case diary and chargesheet.

This handbook uses BNS, BNSS and BSA as the primary legal framework. Older IPC, CrPC and Indian Evidence Act references are retained only where historical case-law, legacy FIRs or pre-1 July 2024 procedural context require them.

History and Role of I4C

The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, Government of India, is the national coordination centre for a comprehensive and coordinated response to cybercrime. I4C supports State and Union Territory LEAs in prevention, detection, investigation and prosecution of cybercrimes. It is a coordination, facilitation, analytical and capacity-building mechanism; investigation and prosecution remain with the competent State/UT Police and legally empowered authorities.

I4C's operationalisation gained impetus after the Supreme Court's directions in In Re: Prajwala Letter Petition concerning circulation of rape videos and online child sexual exploitation material. I4C supports reporting and coordinated handling of Child Sexual Exploitation and Abuse Material (CSEAM), rape/gang rape content, sexually explicit material and other cybercrimes targeting women and children.

NCRP, 1930 and Partner Bodies

The National Cyber Crime Reporting Portal (NCRP) at cybercrime.gov.in is a centralised national reporting platform. Complaints are routed to the concerned State/UT LEA. The 1930 helpline enables immediate reporting by phone through State/UT call centres, especially where the victim cannot visit a police station. Sensitive categories involving women and children may be reported with privacy safeguards, including anonymous reporting where available.

सत्यमेव जयते
Indian Cyber Crime Coordination Centre
सहकार्य करवावे • Working Together With Vigour
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

The National Commission for Protection of Child Rights (NCPCR) monitors child protection laws, issues advisories and supports child online safety. State Commissions for Protection of Child Rights (SCPCRs) perform similar functions at State level. CERT-In provides technical support in cybersecurity incidents, Childline 1098 supports children in distress, and recognised NGOs may assist with counselling, shelter, rehabilitation and court support. These bodies strengthen the protection, reporting, referral and rehabilitation chain.

राष्ट्रीय बाल अधिकार संरक्षण आयोग
भविष्यो रक्षति रक्षितः
NCPCR

certin
Handling Computer Security Incidents

CHAPTER 1

UNDERSTANDING TYPES OF ONLINE CRIMES AGAINST WOMEN & CHILDREN

Online crimes targeting women and children exploit the anonymity, reach, and permanence of digital communications. The categories below are not mutually exclusive — many crimes involve overlapping conduct and applicable law.

1.1 Cybercrimes Targeting Women

The following offences disproportionately target adult women and pose distinct harms:

Offence	Description	Key Provisions
Cyberstalking & Harassment	Repeated, unwanted digital contact to cause fear or distress. Includes persistent messages, GPS tracking, impersonation.	*Sec. 78 BNS; Sec. 66C, 66E IT Act*
Non-Consensual Intimate Images (NCII)	Publishing or threatening to publish private sexual images without consent to humiliate or coerce. Also called image-based sexual abuse.	*Sec. 67A IT Act; Sec. 77 BNS*
Online Sexual Harassment	Sending unsolicited sexually explicit content, obscene messages, or making sexual demands via digital platforms.	*Sec. 67 IT Act; Sec. 75 BNS*
Sextortion	Obtaining sexual images through deception then threatening disclosure unless further content or money is provided.	*Sec. 67A IT Act; Sec. 308 BNS*
Identity Theft & Morphing	Creating fake profiles or digitally altering victim's image into obscene content to damage reputation or blackmail.	*Sec. 66C, 66D, 67 IT Act; Sec. 319/336 BNS as applicable*
Doxxing	Publishing private personal information (address, workplace, family details) online to facilitate harassment or physical harm.	*Sec. 66E IT Act; Sec. 78/351 BNS as applicable*
Online Matrimonial / Romance Fraud	Deceiving victims on matrimonial or dating apps for financial gain, sexual exploitation, or trafficking.	*Sec. 316/318 BNS; Sec. 66D IT Act*

1.2 Cybercrimes Targeting Children

Children are uniquely vulnerable due to their developmental stage, limited digital literacy, and susceptibility to adult manipulation. The following offences specifically target minors:

Offence Type	Description	Key Provisions
Child Sexual Exploitation and Abuse Material (CSEAM)	Production, distribution, storage, viewing, requesting or re-circulation of sexually explicit content involving minors.	*Sec. 14, 15 POCSO; Sec. 67B IT Act*

Offence Type	Description	Key Provisions
Online Grooming	Adult building trust with a child to facilitate sexual abuse via social media, gaming platforms, or messaging apps.	*Sec. 11(ii), 12 POCSO; Sec. 67B IT Act*
Cyberbullying of Minors	Repeated harassment, threatening, or humiliation of a child through digital platforms.	*Sec. 67 IT Act; Sec. 351/352 BNS*
Online Trafficking	Using digital platforms to recruit or facilitate trafficking of children for labour or sexual exploitation.	*Sec. 140/141 BNS; ITPA*
Luring / Enticement	Using the internet to persuade a minor to meet in person for sexual purposes.	*Sec. 11, 12 POCSO; Sec. 67B IT Act*
Live Streaming of Abuse	Broadcasting sexual abuse of a child in real time over the internet to paying viewers.	*Sec. 67A, 67B IT Act; Sec. 14 POCSO*
Dark Web Exploitation	Accessing or trading CSEAM via Tor networks, encrypted channels, and dark web marketplaces.	*Sec. 67B IT Act; Sec. 14, 15 POCSO*

1.3 Emerging & Hybrid Crime Categories

Technological evolution continuously generates new offence modes that may not be explicitly codified but fall within existing statutory ambit through judicial interpretation:

- **Deepfake Sexual Content:** AI-generated or synthetically generated sexual media placing a real person in fabricated sexual scenarios. Sec. 67A IT Act; Sec. 77 BNS by analogy; IT Rules 2026 obligations may apply to intermediary handling.
- **AI-Enabled Grooming:** Use of AI chatbots or generated personas to groom children at scale. POCSO + IT Act framework applies.
- **Metaverse / VR Assault:** Simulated sexual assault in virtual reality environments causing psychological harm. BNS sexual harassment and intimidation provisions may apply depending on facts.
- **Cyber-Enabled Trafficking:** Dark web recruitment, encrypted channels, cryptocurrency payments. BNS trafficking provisions + IT Act + PMLA may apply.
- **Sextortion Syndicates:** Organised networks targeting victims via fake dating profiles. BNS extortion/cheating/intimidation + IT Act + Prevention of Money Laundering Act may apply.

CHAPTER 2

LEGAL & INTERNATIONAL FRAMEWORK

India's legal architecture for combating OCWC is multi-layered, drawing from criminal law, specialised legislation, and international obligations.

2.1 Indian Legislative Framework — Overview

Legislation	Year	Primary Relevance to OCWC
Information Technology Act	2000/2008	Cybercrimes, electronic evidence, CSEAM, obscenity, hacking
Bharatiya Nyaya Sanhita (BNS)	2023	Harassment, stalking, trafficking, obscenity, fraud
POCSO Act	2012	Sexual offences against children, grooming, CSEAM
Indecent Representation of Women Act	1986	Online obscene representation of women
Protection of Women from DV Act	2005	Cyber-enabled domestic violence situations
ITPA (Immoral Traffic Prevention Act)	1956	Trafficking facilitated through online means
Digital Personal Data Protection Act	2023	Consent violations, data misuse enabling crimes
Juvenile Justice Act	2015	Child victims and offenders in digital crimes
BNSS 2023	2023	FIR, investigation, production orders, chargesheet, trial procedure
BSA 2023	2023	Electronic evidence, admissibility, certification and proof

2.2 Key BNS Provisions

BNS Section	Offence	Operational Use	Punishment
74/75	Assault or criminal force to woman; sexual harassment	Online sexual demands, obscene messages, threats linked to sexual conduct	As prescribed
77	Voyeurism	Recording, sharing or threatening to share private images/videos	1-7 years
78	Stalking	Repeated digital contact, monitoring, following or contacting despite disinterest	Up to 5 years
140/141	Trafficking	Online recruitment, transport or exploitation networks	7 years to life
63-70	Rape / aggravated sexual offences	Sexual assault cases with digital facilitation or recording	10 years to life
294	Obscene material	Obscene content where IT Act/POCSO is also examined	As prescribed
351/352	Criminal intimidation / insult	Threats to publish content, threats to victim/family	As prescribed
318/319	Cheating / cheating by personation	Fake profiles, romance fraud, impersonation	As prescribed
308	Extortion	Sextortion demands for money, further images, or sexual acts	Up to 10 years
336/340	Forgery / forged electronic record	Morphed images, fabricated records, forged profiles	As prescribed

2.3 POCSO Act, 2012 — Key Provisions

The Protection of Children from Sexual Offences Act is the primary legislation protecting minors under 18 years from sexual abuse, including that perpetrated through digital means. The POCSO (Amendment) Act 2019 strengthened penalties.

- **Section 11 & 12:** Sexual harassment of a child, including online contact, sending messages, images, or electronic communications.
- **Section 13 & 14:** Use of child for pornographic purposes; production of CSEAM. Punishment: 5–7 years rigorous imprisonment.
- **Section 15:** Storage of pornographic material involving a child — imprisonment up to 3 years or fine or both.
- **Section 19:** Mandatory reporting obligation — any person with knowledge of an offence under POCSO must report to the SJPU or local police.
- **Section 20:** Media obligation not to disclose identity of child victim.
- **Section 33 & 36:** Special Court provisions; child-friendly recording of evidence; camera trial.
- **Section 42-A:** POCSO overrides BNS where inconsistent — ensures higher punishment applies.

Critical Note: *Under POCSO, consent of a minor is legally irrelevant. Any sexual activity involving a person below 18 years constitutes an offence, regardless of claimed consent.*

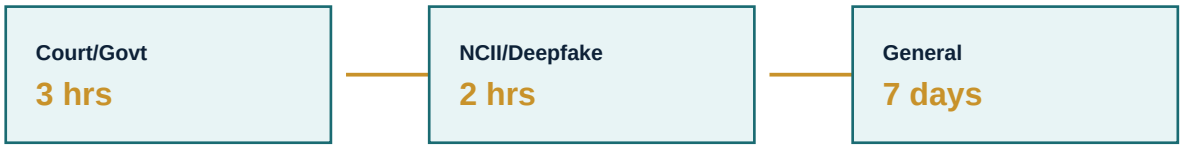
2.4 IT Act 2000 — Key Sections for OCWC

Section	Offence	Punishment
Sec. 66C	Identity theft	Up to 3 years + fine up to Rs. 1 lakh
Sec. 66D	Cheating by personation using computer resources	Up to 3 years + fine up to Rs. 1 lakh
Sec. 66E	Violation of privacy (publishing private images)	Up to 3 years + fine up to Rs. 2 lakh
Sec. 67	Publishing obscene material electronically	Up to 3–5 years + fine
Sec. 67A	Publishing sexually explicit material electronically	Up to 5–7 years + fine
Sec. 67B	Publishing CSEAM / child sexual abuse material	Up to 5–7 years + fine
Sec. 69	Government interception/monitoring of information	Procedural — relevant for lawful evidence gathering
Sec. 72	Breach of confidentiality and privacy	Up to 2 years + fine
Sec. 79	Safe harbour for intermediaries — conditions for immunity	Procedural — affects notice & takedown

2.5 IT Rules 2021 as Amended in 2026

The Union Government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 on 10 February 2026, effective 20 February 2026. For OCWC work, the amendments are operationally important because they shorten takedown timelines for unlawful and sexually exploitative material, define obligations around synthetically generated information (SGI), and strengthen grievance response expectations for intermediaries.

IT Rules 2021 - Amendment 2026 Takedown Timelines



Trigger	Old Timeline	New Timeline	Rule
Court order or reasoned Government order for unlawful content	36 hours	3 hours	Rule 3(1)(d)
Grievance involving nudity, sexual acts, impersonation, morphed images, deepfake sexual content or NCII	24 hours	2 hours	Rule 3(2)(b)
General user grievances	15 days	7 days	Grievance redressal

LEA use: *In urgent OCWC matters, secure evidence first, then initiate takedown through lawful channels. Do not wait for content to disappear before recording URLs, handles, hashes, screenshots, metadata and platform identifiers. Full rules/FAQ: https://i4c.pages.dev/itact*

Scan for IT Rules 2026 FAQ
https://i4c.pages.dev/itact

2.6 BSA and BNSS: Evidence and Procedure

The Bharatiya Sakshya Adhiniyam, 2023 replaces the Indian Evidence Act for the proof of electronic records. Section 63 of the BSA governs admissibility of electronic records and the required certificate. The certificate should identify the electronic record, explain how it was produced, confirm the device/system details, and be completed by the person responsible for the device/system or an expert as applicable. The IO should obtain the certificate at the earliest stage, preferably from the platform, service provider, FSL, or person operating the relevant computer resource.

The BNSS is the primary procedural code for FIR registration, production orders, search, seizure, arrest, remand, chargesheet and trial process. Use BNSS production powers for ISPs/intermediaries and record each request, response, reminder and non-response in the case diary. Where older judgments mention legacy evidence or production provisions, translate the operational requirement to BSA Section 63 and the corresponding BNSS production process.

2.7 Digital Personal Data Protection Act, 2023

- Processing of personal data of children requires verifiable parental consent (Section 9).
- Data fiduciaries are prohibited from tracking, behavioural monitoring, or targeting advertising at children.
- Victims' personal data collected during investigation is subject to strict data minimisation norms.
- Violation of data protection norms enabling criminal conduct may attract DPDP penalties alongside IT Act liability.

2.8 International Frameworks & Conventions

Budapest Convention on Cybercrime (2001)

The primary international treaty on cybercrime. Relevant for cross-border CSEAM and NCII cases.

UN Convention on the Rights of the Child (UNCRC)

India ratified UNCRC in 1992. Optional Protocol on Sale of Children (OPSC) criminalises CSEAM.

Interpol Cooperation

NCIB India coordinates with Interpol through Operations Rescue, Koala for CSEAM investigations. ICSE database enables victim identification.

MLAT Framework

Mutual Legal Assistance Treaties enable India to seek and provide evidence from foreign jurisdictions.

Lanzarote Convention (2007)

Protection of children against sexual exploitation — India engages through UN mechanisms.

FATF Guidance

Detecting and disrupting financial flows associated with child sexual exploitation and sextortion syndicates.

CHAPTER 3

INVESTIGATION & PROSECUTION

Effective investigation of OCWC requires a structured, victim-centred, evidence-first approach. This chapter provides step-by-step operational guidance for law enforcement officers.

3.1 FIR Registration — Procedure & Jurisdiction

Registration of the FIR is the gateway to formal criminal proceedings. In cyber crimes against women and children, FIR registration requires particular care given the cross-jurisdictional and electronic nature of the offence.

Who Can Register?

- The victim herself/himself (or parent/guardian for minor victims).
- Any person on behalf of the victim if she/he is unable to do so (BNSS provisions on information to police and FIR registration).
- NCPCR, SCPCR, or NGOs recognised under JJ Act may also assist in filing.

Jurisdiction Considerations

- Cyber crimes may be registered at any police station; jurisdiction should not delay registration or emergency action.
- For online crimes, the offence is considered committed where the message/content was received or viewed.
- Dedicated Cyber Crime Police Stations (CCPS) have concurrent jurisdiction.
- The National Cyber Crime Reporting Portal (cybercrime.gov.in) enables online complaint filing.

FIR Drafting — Key Elements to Include

- Complete description of the offending conduct — what was posted/sent/shared and how.
- URLs, platform names, account handles/usernames, email IDs of the offender (if known).
- Date and time of first knowledge of the offence.
- Screenshots or evidence already in victim's possession.
- Full details of victim — name, contact, and for minors, guardian details.
- Statement that the victim has not given consent to publication/sharing.
- Relief sought: removal of content, arrest of accused, preservation of records.

Zero FIR: *A police officer should not refuse registration on jurisdictional grounds. Register, preserve evidence, initiate urgent takedown, and transfer to the competent police station as required.*

POCSO Cases: The Special Juvenile Police Unit (SJPU) must be informed within 24 hours. Child statement must be video-recorded under Sec. 26 POCSO in a child-friendly environment.

3.2 Sections to be Invoked — Quick Reference Matrix

The following matrix maps crime types to recommended sections. Officers should invoke all applicable sections to ensure the chargesheet is solid.

Crime Type	IT Act	BNS	Special Act
Cyberstalking	66C, 66E	Sec. 78	-
NCII / Revenge Porn	66E, 67A	Sec. 77/351 as applicable	-

Crime Type	IT Act	BNS	Special Act
Online Sexual Harassment	67, 66E	Sec. 75	-
Sextortion	66D, 67A	Sec. 308/351	-
Morphing	66D, 67	Sec. 336/340	-
CSEAM (Production)	67B	-	Sec. 13, 14 POCSO
CSEAM (Storage/Viewing)	67B	-	Sec. 15 POCSO
Online Grooming	67B	-	Sec. 11, 12 POCSO
Online Trafficking	66D	Sec. 140/141	ITPA Secs. 4-6
Impersonation / Fake Profile	66C, 66D	Sec. 318/319	-
Cyberbullying (Minor)	66, 67	Sec. 351/352	JJ Act Sec. 75

3.3 Steps for Evidence Collection

A. Immediate Steps (Within First 48 Hours)

- Secure and preserve all devices in the victim's possession — do not allow factory reset or deletion.
- Take screenshots of offending content before it is taken down.
- Preserve metadata of all messages, images, or emails — do not forward without noting timestamps.
- Send preservation request to the platform (Google, Meta, Twitter/X) via abuse portal.
- Issue BNSS production order to ISPs/intermediaries for IP logs, subscriber details and preservation.
- Contact CERT-In for critical infrastructure involvement or cross-border hosting.

B. Intermediate Steps (Investigation Phase)

- Obtain court order for interception/monitoring if real-time tracking needed (Sec. 69 IT Act).
- Issue notice to intermediary platforms under Sec. 79 IT Act for traceability data.
- Coordinate with NCMEC CyberTipline for CSEAM - reports routed through NCIB/I4C channels as applicable.
- Seize server logs, CCTV footage, access records from cyber cafés or shared networks.
- Identify and secure all suspect digital devices — mobile phones, laptops, drives.
- Prepare device seizure memo and BSA Section 63 electronic evidence certificate workflow.
- Conduct forensic imaging of seized devices using write-blockers.

3.4 Digital Evidence Collection — Forensic Standards

Digital evidence must be collected, preserved and produced in compliance with the BSA and established cyber forensic standards. Failure to follow proper chain of custody can render evidence inadmissible or reduce its probative value.

Types of Digital Evidence in OCWC Cases

Evidence Type	Key Considerations
Communication Logs	WhatsApp chats, SMS, emails, DMs — export in original format with timestamps.
Social Media Content	Posts, stories, profiles, friend/follower lists, account data.

Evidence Type	Key Considerations
Images & Videos	Offending content with EXIF data intact — do NOT re-compress.
Device Artefacts	Browser history, app logs, call logs, deleted data recovered via forensic tools.
Network Evidence	IP address logs, DHCP records, VPN logs, Wi-Fi router logs.
Financial Trails	UPI transaction IDs, cryptocurrency wallet addresses, payment logs.
Cloud Storage	Google Drive, iCloud, OneDrive backups — require production orders / MLAT.
Email Headers	Full raw email headers reveal sender IP, routing, timestamp.

BSA Section 63 Certificate Requirement

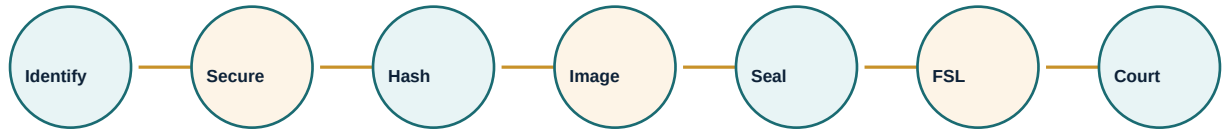
Electronic evidence should be accompanied by a certificate under Section 63 BSA 2023, signed by a responsible official or competent expert attesting to authenticity, integrity, source system details and the manner in which the electronic record was produced.

Legacy case-law note: *Anvar P.V. and Arjun Panditrao dealt with BSA Section 63 of the Indian Evidence Act. For current filings, map the same admissibility discipline to BSA Section 63 and obtain the certificate as early as possible.*

Chain of Custody Documentation

- Each piece of evidence must be sealed in a tamper-evident evidence bag with unique exhibit number.
- Chain of Custody form must record every person who handled evidence, with date/time/purpose.
- Forensic hash values (MD5/SHA-256) must be computed at seizure and verified before/after examination.
- Forensic examination conducted on verified forensic images — never on original devices.
- All forensic tools used must be validated, licensed, and documented.

Digital Evidence Chain of Custody



Record handler, date/time, purpose, seal number, hash and transfer at every stage.

Scan for Chain of Custody SOP
https://i4c.pages.dev/coc

Court submission: *Attach seizure memo, hash sheet, BSA Section 63 certificate, FSL report, transfer log, platform response, and exhibit index. Every exhibit in the chargesheet should map to a witness and a fact in issue.*

3.5 Victim Statements & Victim Identification

Recording Victim Statements

Victim statements are the cornerstone of OCWC prosecutions. Must be recorded with sensitivity, accuracy, and strict procedural compliance.

- Female victims should be examined by a female officer whenever possible under BNSS victim-sensitive procedure.
- Child statements must be video-recorded under Sec. 26 POCSO in a child-friendly environment.

- Use an interpreter if victim has communication barriers.
- Do not record statement in presence of accused or hostile environment.
- Obtain detailed written account: timeline, platforms used, nature of contact, impact.
- Magisterial statement under BNSS: essential if the complainant may turn hostile or the facts are sensitive.

Victim Identification Protocols

- NCMEC CyberTipline reports contain victim ID data — coordinate with NCIB.
- Interpol's ICSE database enables victim identification from CSEAM hashes.
- Social media OSINT can help locate and identify groomed or trafficked minors.
- In NCII cases, reverse image search tools may help identify victim.
- Victim anonymity must be preserved — no disclosure of name/address (POCSO Sec. 23 and applicable identity-protection provisions).
- Conduct risk assessment for victim safety before public action.

3.6 Preparation of a Fool-Proof Chargesheet

The chargesheet must present a complete, legally sound, evidence-backed narrative that withstands scrutiny at trial.

Essential Components

- **Cover Page:** Case number, police station, sections, accused details, court details.
- **Synopsis of Facts:** Clear, chronological narrative — plain language, free of assumptions.
- **Section-wise Charges:** Each count with section, offence description, date, and evidence linking accused.
- **Witness List:** PW1=victim, PW2=IO, PW3=forensic examiner — with full addresses.
- **Exhibit List:** All documentary and electronic evidence with exhibit numbers and BSA Section 63 certificates.
- **Forensic Reports:** FSL report, cyber forensic examination report, CDR analysis.
- **Accused Details:** Full particulars, photograph, prior criminal history, bail status.
- **Victim Statement Summary:** Gist of Sec. 161 and 164 statements — do not reproduce full text.
- **IO's Certificate:** Certifying investigation complete or supplementary chargesheet to follow.

Common Deficiencies to Avoid

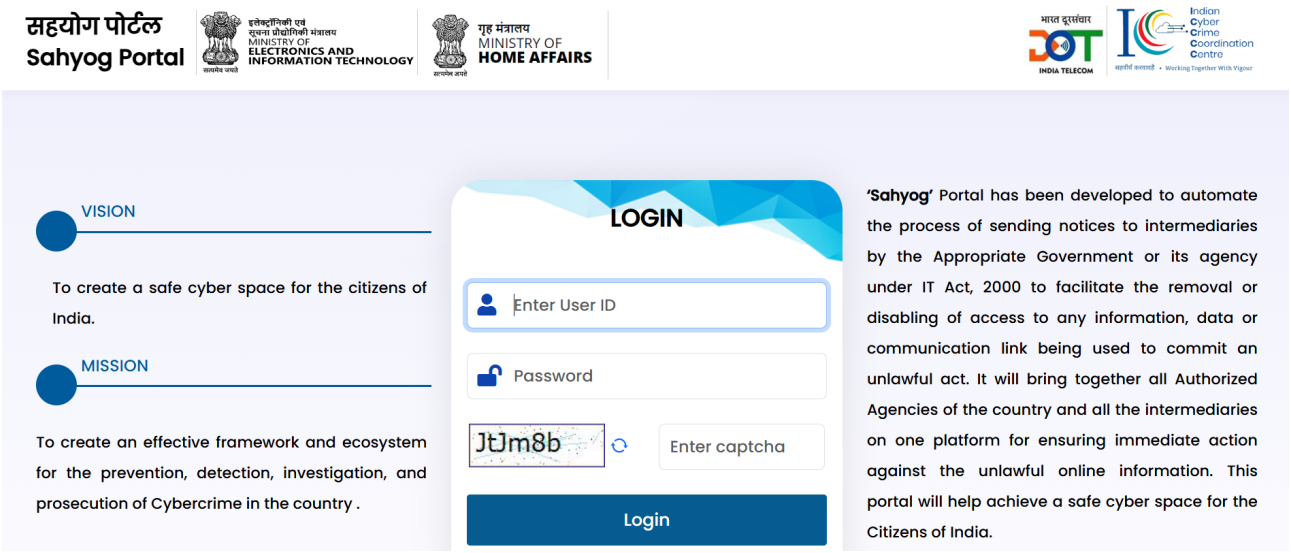
- Missing or defective BSA Section 63 certificate — renders all electronic evidence inadmissible.
- No specific digital evidence linking accused to device/account used.
- Charge sections not matching recovered evidence — over/under-charging.
- Incomplete FSL report — submit supplementary if analysis pending.
- Victim's identity disclosed in chargesheet — must be anonymised.
- Failure to implead all accused including abetters and platforms.

Supplementary Chargesheet: If investigation ongoing or evidence pending (MLAT response, forensic report), file initial chargesheet with available evidence and follow with supplementary. Failure to file within the prescribed period may lead to default bail under BNSS.

3.7 NCRP, 1930, Sahyog and Urgent Takedown

Immediate securing and removal of objectionable content is a top priority in OCWC cases. The IO should first preserve evidence, then move quickly for removal so the victim is protected from continuing harm. A takedown request without preservation may weaken trial; preservation without takedown may prolong victimisation. Both must move together.

- For citizens: guide the victim/guardian to cybercrime.gov.in and 1930 for reporting and acknowledgement number generation.
- For LEAs: use Sahyog for lawful notices, takedown requests, preservation requests and platform coordination where the agency is authorised/onboarded.
- For platform data: send URL, account ID, channel ID, phone/email identifier, hash value, FIR/complaint reference, legal provision and urgency reason.
- For no response: record timestamped reminders, escalate to the designated grievance/nodal officer, and document non-compliance in the case diary.
- For Section 94 BNSS/production responses: keep ISP, intermediary and platform responses in separate indexed bundles with request-response timelines.



Scan for Sahyog Portal
https://sahyog.mha.gov.in

Sahyog Portal - LEA Use

The Sahyog Portal, developed under I4C, is a restricted coordination platform for authorised LEAs, intermediaries, ISPs, VASPs and other authorised entities. It is not a public complaint portal. Public complaints should generally be filed through NCRP; authorised agencies may then process notices, preservation and takedown requests internally through Sahyog.

Sahyog can support URL takedown, account or channel-based requests, hash-sharing for CSEAM/NCII, preservation of logs and subscriber information, and a documented compliance trail. Where intermediaries do not respond, the IO should separate no-reply cases from replies received under BNSS production requests, preserve screenshots of dashboard/email status, and escalate through official channels to the grievance officer or nodal contact.

3.8 Raid Scene Protocol When No Cyber Expert Is Present

- Do not browse, open, forward, delete, rename, factory reset, or plug seized devices into police systems.
- Photograph the scene, device screens, connections, power state, SIM slots, routers and storage media before movement.
- If a device is on and unlocked, note visible state, keep it powered if volatile evidence is likely, and seek remote expert guidance.
- If a device is off, do not turn it on. Pack, seal and label it with date, time, place, witness and officer details.

- Isolate phones from networks using airplane mode/Faraday bag only after documenting screen state where possible.
- Seize routers, DVRs, external drives, memory cards, notebooks with passwords, and payment instruments linked to the offence.
- Prepare a device-wise seizure memo and hand over promptly to a cyber cell/FSL for forensic imaging with hash values.

3.9 Age Determination, Rehabilitation and Monitoring

Age Determination of Child Victim

Age determination is decisive in CSEAM and online grooming cases because the victim may not be physically present at the first reporting stage; the case may begin from a video, image, hash match or CyberTipline report. Failure to prove the victim was below 18 can lead to acquittal even where the digital content is recovered.

- Collect birth certificate, school admission register, Aadhaar/passport where legally usable, hospital birth record, immunisation record, or CWC/JJ records.
- Record guardian statement explaining identity and age documents; verify issuing authority where needed.
- Where identity is unknown, use victim identification protocols, hashes, facial clues, background clues, metadata, platform records and inter-state coordination.
- If documentary age proof is unavailable or disputed, seek medical age opinion through the legally appropriate board and record limitations.
- Link each age document to the seized image/video through victim identification witness, forensic report, platform record or recovery memo.

Forensic Child Counsellor and Support Persons

In child cases, the IO should coordinate with the CWC/DCPU/SJPU for appointment of a support person, counsellor, interpreter, special educator or mental health professional as needed. Prefer professionals with child psychology, social work, psychiatry, clinical psychology, counselling or child protection experience, and avoid repeated interviewing by untrained persons. The counsellor supports the child; the IO remains responsible for lawful investigation.

Victim Compensation and Rehabilitation

- Inform victim/guardian about State Victim Compensation Scheme, NALSA/SLSA/DLSA support and POCSO victim compensation routes.
- Refer child victims to CWC/DCPU for care plan, shelter, counselling, medical care, education continuity and family risk assessment.
- Use One Stop Centre, Women Helpline 181/1091, Childline 1098, hospital crisis centres and approved NGOs for immediate support.
- Where available, guide victims to State emergency/safety applications and local cyber volunteer or women safety cells.
- Record referrals in the case diary and follow up; rehabilitation evidence can support impact assessment and sentencing.

Conviction Rate: Why Cases Fail and How to Fix Them

Gap	Practical Fix
No age proof in child cases	Collect and verify age documents early; link them to the digital content and victim identity.
Weak electronic evidence certificate	Use BSA Section 63 certificate from source/system owner/FSL/platform as applicable.
No accused-device-account link	Correlate device seizure, IP logs, CDR, subscriber records, platform login logs and recovery.
Delayed preservation	Send preservation/takedown and production requests immediately; record all timestamps.
Victim identity disclosure	Use anonymised filing, sealed covers where needed, and POCSO Sec. 23 compliance.
Poor chain of custody	Use exhibit numbers, seals, hashes, transfer logs, FSL receipt and court exhibit mapping.

Performance Monitoring and Escalation to I4C

Each OCWC unit should maintain a dashboard of FIRs, NCRP acknowledgements, 1930 calls, takedown requests, Sahyog notices, intermediary replies/no replies, FSL pendency, age proof status, BSA certificate status, chargesheet due date and victim support referrals. Where field officers face recurring technical or intermediary coordination issues, the supervisory officer may escalate through official I4C/State cyber coordination channels with complaint number, FIR number, URLs/hashes, request IDs and action already taken.

CHAPTER 4

IMPORTANT HC/SC JUDGEMENTS & KEY TAKEAWAYS

Indian courts have significantly shaped OCWC jurisprudence through landmark judgements. This chapter consolidates precedents with practical implications for investigators and prosecutors.

4.1 Supreme Court Landmark Judgements

■ In Re: Prajwala Letter Petition

Supreme Court of India

Issue	Circulation of rape videos and child sexual exploitation material online.
Held	The Court pressed for institutional reporting and coordinated handling of online sexual offences against women and children.
Key Takeaway	**Use I4C/NCRP coordination channels, preserve evidence, and pursue prompt takedown for CSEAM and RGR content.**

■ Just Rights for Children Alliance v. S. Harish

Supreme Court of India, 2024

Issue	Possession, viewing, retention or failure to delete/report CSEAM.
Held	Possession or constructive possession of CSEAM may attract criminal liability; intent may be inferred from conduct.
Key Takeaway	**Investigate storage, viewing history, downloads, cache, cloud sync and failure to report/delete; do not treat mere non-upload as harmless.**

■ Aparna Bhat & Ors. v. State of Madhya Pradesh

(2021) 5 SCC 1

Issue	Victim dignity and bail conditions in sexual offence cases.
Held	Courts cannot impose compromise-oriented or victim-contact conditions that undermine dignity.
Key Takeaway	**Oppose bail terms that expose the victim to accused contact, pressure or further circulation of content.**

■ Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

(2020) 7 SCC 1

Issue	Electronic evidence certification discipline under the legacy Evidence Act.
Held	Electronic records require proper certification from the person/system responsible, subject to recognised exceptions.
Key Takeaway	**For current cases, apply the same discipline through BSA Section 63 and collect certificates early.**

4.2 High Court Notable Orders

■ Rajesh Gambhir v. State (NCT of Delhi)

Delhi High Court, 2025

- **Facts/Held:** Morphing of images, cyberstalking and threats against a minor were treated as digital sexual exploitation attracting IT Act, BNS and POCSO provisions.

Practitioner Takeaway: *In morphing/deepfake cases, preserve source files, edited files, handles, threat messages and accused-device linkage.*

■ X v. Union of India

Madras High Court, 2025

- **Facts/Held:** Court emphasised prompt takedown and intermediary responsibility to prevent continuing circulation of objectionable content.

Practitioner Takeaway: *Do not wait for trial to seek removal; secure evidence, then move takedown and preservation in parallel.*

■ Court on its Own Motion v. State & Ors.

Delhi High Court

- **Facts/Held:** Directions focused on strengthening institutional mechanisms and coordinated response to online sexual exploitation.

Practitioner Takeaway: *Use institutional coordination: cyber cell, CWC/SJPU, I4C/NCRP, platform nodal officers and victim support services.*

■ State of West Bengal v. Animesh Boxi

Calcutta HC, 2018 | NCII / Revenge Porn

- **Facts/Held:** Accused uploaded obscene images of victim on Facebook/WhatsApp. HC: posting intimate images without consent = offence under Sec. 67A IT Act and Sec. 77 BNS.

Practitioner Takeaway: *First HC ruling on NCII as standalone offence. Sec. 354C voyeurism extends to digital recording and sharing without consent.*

■ Kamlesh Vaswani v. Union of India (PIL)

Supreme Court, 2014 | CSEAM

- **Facts/Held:** PIL seeking ban on child pornography websites. SC: directed DoT to block identified CSEAM URLs and establish nodal agency.

Practitioner Takeaway: *Established government obligation to proactively block CSEAM. Contributed to NCMEC/NCIB coordination framework.*

■ X v. Union of India (Revenge Porn PIL)

Delhi HC, 2021

- **Facts/Held:** HC acknowledged gap in legislation for NCII. Directed government to consider dedicated legislation. Interim directions for expedited takedown.

Practitioner Takeaway: *Judicial recognition of NCII as distinct harm requiring statutory remedy. Useful for bail denial and injunctive relief.*

■ Cyberbullying — Minor Victim (Writ Petition)

Karnataka HC, 2019

- **Facts/Held:** HC: school authorities aware of cyberbullying incidents among students cannot plead ignorance — school has duty of care extending to digital environments.

Practitioner Takeaway: *Relevant for institutional duty — schools, platforms, employers. Supports ancillary civil remedies alongside criminal prosecution.*

4.3 Consolidated Key Takeaways for Practitioners

Evidence

- Always obtain BSA Section 63 certificate contemporaneously with seizure — cannot be supplied later.
- Hash all digital evidence immediately — tampering is immediately detectable.
- Forensic imaging is non-negotiable — never examine original devices.

FIR & Jurisdiction

- Zero FIR / jurisdiction-neutral registration should be used so emergency preservation and takedown are not delayed.
- Preserve platform data before filing — platforms purge logs within 30–90 days.
- Cyber crimes registered at any police station regardless of physical location.

Victim Protection

- Victim identity never disclosed — failure is itself an offence (POCSO Sec. 23 and applicable identity-protection provisions).
- Bail conditions cannot involve victim — Aparna Bhat guidelines binding on all courts.
- Assess victim safety risks before enforcement action.

POCSO Specifics

- Consent of a minor is irrelevant — any sexual content involving under-18 is absolute offence.
- Mandatory reporting under Sec. 19 POCSO extends to all citizens, not just police.
- Video-record all child statements — failure may lead to acquittal.

Platforms & Intermediaries

- Section 66A is dead — do not invoke. Use Sec. 67, 67A, 67B instead.
- NCMEC CyberTipline is fastest route for CSEAM takedown on US-based platforms.
- Platforms liable only after court/government notice — but preservation requests sent immediately.

ANNEXURES

Annexure A — Emergency Contact & Reporting Portals

Portal / Helpline	Contact	Purpose
National Cyber Crime Reporting Portal	cybercrime.gov.in	Online complaint filing — all cyber crimes
Cyber Crime Helpline	1930	Immediate cyber crime reporting
Women Helpline	181 / 1091	Women in distress
Child Helpline	1098 (Childline)	Children in danger / exploitation
NCMEC CyberTipline	cybertipline.org	CSEAM reporting from India
CERT-In	cert-in.org.in	Critical infrastructure / national-level incidents
NCIB (Interpol India)	Via CBI	International cases / CSEAM cross-border
Meta/Facebook Reporting	facebook.com/help	NCII / harassment on Meta platforms
Google Safety Centre	google.com/safetycenter	Content removal — Google platforms

Annexure B - ISP, Telecom and Network Provider LEA Contacts

Under the Information Technology Rules, 2021, intermediaries maintain grievance/nodal contacts for takedown notices, data requests and lawful communications. Because LEA/legal desks may change internally, role-based institutional emails such as nodal@, lea@ and grievance@ should be preferred. Verify the latest provider contact page or Sahyog/onboarded directory before issuing time-sensitive notices.

Submission protocol: *Formal takedown or data requests should originate from an official government/law-enforcement domain where possible, include FIR/complaint reference, legal provision, exact URLs/account IDs/hashes, preservation period requested, officer contact and certified court/government order where required.*

Tier 1 & Pan-India Providers

S.No	Service Provider	Grievance / Nodal Contact	Legal Desk / LEA / Takedown Email
1	Reliance Jio Infocomm	Nodal Officer Desk	jio.nodalofficer@ril.com / lea.support@jio.com
2	Bharti Airtel	Nitin Grover / Seema Jindal	Content.Grievance@airtel.com / nodalofficer@airtel.com
3	Vodafone Idea (Vi)	Rahul Gupta / Nodal Desk	contentregulation.vimoviesandtv@vodafoneidea.com / nodal.officer@vodafoneidea.com
4	BSNL	Sh. Vishwa Mohan (DDG Reg)	ddg_reg@bsnl.co.in / vishwamohan@bsnl.co.in
5	MTNL	Public Grievance Desk	pgmregco@mtnl.net.in / nodalofficer.delhi@mtnl.net.in
6	Tata Communications / Tata Play	Regulatory Compliance Team	nodal.officer@tatacommunications.com / legaldesk@tataplayfiber.co.in

Major Regional Broadband & Fiber ISPs

S.No	Service Provider	Grievance / Nodal Contact	Legal Desk / LEA / Takedown Email
7	ACT Fibernet	Hosabettu Venkatesh Bhat	nodalofficer@actcorp.in / legal.desk@actcorp.in
8	Hathway Cable & Datacom	Nodal Compliance	nodalofficer@hathway.net / legal@hathway.net
9	Siti Broadband	Grievance Officer	grievance.broadband@sitinetworks.com
10	Alliance Broadband	Arunabha Banerjee	arunabha@alliancekolkata.com / legal@alliancebroadband.co.in

S.No	Service Provider	Grievance / Nodal Contact	Legal Desk / LEA / Takedown Email
11	Excitel Broadband	Legal Compliance Team	compliance@excitel.com / nodal@excitel.com
12	GTPL Hathway	Nodal Desk	nodal.broadband@gtpl.net / grievance@gtpl.net
13	Asianet Satellite Communications	Satish Kumar S.	s_satishkumar@asianet.co.in / nodalofficer@asianet.co.in
14	Tikona Infiniti Private Ltd.	Nodal Compliance Officer	nodalofficer@tikona.in / lea.desk@tikona.in
15	You Broadband (Vodafone Idea)	Compliance Cell	nodalofficer@youbroadband.in
16	Spectra (Connectinside Pvt Ltd)	Nodal Officer	nodal.officer@spectra.co
17	Den Networks	Rajesh Kaushal	nodalofficer@denonline.in / legal@dennetworks.com
18	Fastway Transmissions (Netplus)	Nodal Desk	nodalofficer@netplus.co.in
19	Oneott Intertainment (InDigital)	Grievance & Nodal Cell	nodal.broadband@nxtdigital.in
20	Cherrinet (KNET Solutions)	Regulatory Head	nodalofficer@cherrinet.in
21	Wish Net Pvt Ltd	Compliance Desk	nodalofficer@wishnet.co.in
22	Sify Technologies	Legal Desk	nodalofficer@sifycorp.com
23	Ortel Communications	Nodal Desk	nodalofficer@ortelgroup.com
24	Microsense Private Ltd	Compliance Officer	nodalofficer@microsenseindia.com
25	Mudra Digital	Legal Head	grievance@mudradigital.com

Enterprise, VNO & Cloud Carrier Desks

S.No	Service Provider	Grievance / Nodal Contact	Legal Desk / LEA / Takedown Email
26	AT&T; Global Network India	Naveen Tandon	ntandon@att.com / att-india-regulatory@att.com
27	BT Global Communications	Satyen Gupta	satyen.gupta@bt.com / india.regulatory@bt.com
28	Orange Business Services	Regulatory Desk	india.regulatory@orange.com
29	Verizon Communications India	Compliance Officer	verizon.india.nodal@verizon.com
30	Vodafone Business Services	Corporate Nodal Desk	corporate.nodal@vodafoneidea.com
31	Data Infosys / Data Ingenious	Ajay Kumar Data	grievance@dil.in / ajay@dataone.in
32	RailTel Corporation of India	Vigilance/Grievance Desk	nodalofficer@railtelindia.com
33	PowerGrid Telecom (POWERTEL)	Compliance Desk	powertel_nodal@powergrid.in
34	Pioneer Elabs Ltd	Nodal Officer	nodal@pioneerelabs.com
35	City Online Services Ltd	R.K. Mohan	rkmohan@cityonlines.com / nodal@cityonlines.com
36	Compucom Software Ltd	Surendra Kumar Surana	grievance@compucom.co.in
37	Conjoinix Technologies	Nitish Mahajan	legal@conjoinix.com
38	Blazenet Ltd	Sharad Varia	sharad@blazenet.net
39	Broadband Pacenet (I) Pvt Ltd	Regulatory Desk	subramaniyan@pacenet-india.com / legal@pacenet.in
40	Softech Infosol Pvt Ltd	Hardeep Sandhu	hardeepsandhug@gmail.com
41	Esto Broadband	Manish Kumar	info@estobroadband.in
42	Abuse / Registry.in Desk (NIXI)	National Registry Desk	nixi-grievance-officer@nixi.in
43	CSC E-Governance Services	Bhagwati Jamnal	bhagwati.jamnal@csc.gov.in
44	Cyfuture India Private Ltd	Atul Sharma	atul.sharma@cyfuture.com
45	Sinet / Ski Network Services	Himanshu Arora	compliance@skynet.in
46	Advanced Financial Services	Regulatory Desk	vasu@advfin.com
47	Aeroway Networks	Arun Kumar	compliance@aeroway.in
48	Apna Telelink Ltd	Amarjit Singh	as@apnatelelink.com
49	Astro Network India	Compliance Desk	venunath@astronetwork.net
50	Beam Cable System	Regulatory Team	compliance@beamtel.com

Annexure C - OCWC Investigation Checklist

- ■ FIR registered with correct sections; Zero FIR if jurisdiction issue
- ■ SJPU / CWC notified (POCSO cases)
- ■ Victim identity protected — no disclosure in documents
- ■ Victim statement recorded by female officer (if applicable)
- ■ Victim's devices secured and isolated
- ■ Screenshots / screen recordings of offending content taken
- ■ Platform preservation request sent
- ■ BNSS production order issued to ISP/intermediary
- ■ Suspect's devices seized with witnesses
- ■ Forensic hash values computed at seizure
- ■ Forensic imaging of devices (write-blocker used)
- ■ BSA Section 63 certificate obtained
- ■ CDR / IP address records obtained
- ■ BNSS magisterial statement recorded where required
- ■ NCMEC CyberTipline report filed (CSEAM cases)

- Chargesheet filed within prescribed period
- Forensic report annexed to chargesheet
- Victim informed of case progress

This handbook is intended as an operational reference tool for Law Enforcement Agencies and does not constitute legal advice. All statutory references should be verified against the latest gazette notifications. Prepared by I4C | OCWC Handbook for Law Enforcement Agencies | 2026