

“SURVIVOR’S GUIDE: NCII & CSAM REPORTING AND LEGAL RECOURSE”

A Practical Guide for Survivors in India on Reporting, Removal, and Legal Recourse



REPORTING PROCESS:

Clear steps for filing complaints with platforms & authorities



LEGAL RECOURSE:

Understanding rights & utilizing legal mechanisms under Indian law



SUPPORT SYSTEMS:

Accessing helplines, counseling, and NGO assistance

Curated By Reportsentinel & Hackphiles

INDEX

Quick Reference Guide to Survivor Support, Reporting, and Legal Guidance for NCII & CSAM.

1. Cover Page

- SURVIVOR'S GUIDE

2. Immediate Safety & Emotional Support

- Brace for impact, connect with family/friends.
- Do not confront the perpetrator directly.

3. Preserve Evidence

- Take screenshots, save messages and URLs.
- Do not share or forward content.

4. Reporting to Authorities

- National/State Cybercrime portals, escalation process.
- Circulation warning and police station contacts.

5. Content Removal & Trusted Platforms

- Adult/Minor platforms, NGO support for takedown.
- Hash-based removal; content never leaves device.

6. Kerala Police, Cyberdome & CCSE Units

- Contact emails for specialized units.
- One Stop Centres and MeltY NCII SOP details.

7. NGO Support & Counselling

- Emergency support, trauma counselling, legal guidance.
- List of trusted NGOs and helplines.

8. Digital Hygiene & Privacy Safeguards

- Change passwords, enable 2FA, audit devices.
- Adjust privacy settings on all platforms.

9. Trauma & Psychological Support

- Use OSC, private counselors; avoid over-monitoring.
- Join support groups for reducing stress.

10. Explicit Do's & Don'ts

- Visual comparison of recommended actions (Do's).
- Actions to avoid (Don'ts) with reasons.

11. Hard Truths

- Challenges with private channels, law enforcement limits.
- Reality of hash-blocking and circulation.

12. High Court Intervention

- Writ petition steps, sealed records procedure.
- Seeking gag orders for protection.

13. Emergency Helplines & Conclusion

- Childline 1098, Cyber Crime Helpline 1930.
- Summary of SOP and final supportive message.

IMMEDIATE SAFETY & EMOTIONAL SUPPORT

Guidance for immediate actions and well-being.

1. ENSURE IMMEDIATE SAFETY



- ✓ Secure your physical environment.
- ✓ Disconnect from harmful digital platforms.
- ✓ Contact trusted individuals or authorities.
- ✓ Avoid immediate confrontation.
- ✓ Document any threats discreetly.

⚠ Warning: Prioritize your physical safety above all.

2. SEEK EMOTIONAL SUPPORT



- ♥ Reach out to a trusted friend or family member.
- ♥ Connect with a professional counselor or therapist.
- ♥ Join a support group for survivors.
- ♥ Practice calming techniques (breathing, grounding).
- ♥ Allow yourself to feel without judgment.

人群中的人图标 Reminder: You are not alone; support is available.

3. ACCESS PROFESSIONAL GUIDANCE



- Consult legal aid for advice on rights.
- Contact relevant NGO helplines.
- Inform the local police or cyber cell.
- Preserve all evidence (screenshots, URLs).
- Follow official reporting procedures.

i Note: Professional guidance ensures informed decisions.

PRESERVE EVIDENCE

Crucial steps for securing digital and physical proof for reporting.



1. Secure Digital Content

- ✓ Take immediate screenshots of all relevant content, including timestamps and URLs.
- ✓ Save original image/video files without altering metadata.
- ✓ Record platform details, user profiles, and any associated comments or captions.



2. Document All Communications

- ✓ Save chat logs, emails, and message history in their original format.
- ✓ Note down dates, times, and the identities of individuals involved.
- ✓ Keep a log of any communication with platforms or authorities.



3. Store Safely & Securely

- ✓ Create multiple **backups** on secure, offline devices (e.g., USB, external drive).
- ✓ Use **password-protected folders** or **encrypted storage** solutions.
- ✓ Keep physical devices and backups in a secure, private location.

IMPORTANT NOTE



- ✗ **DO NOT DELETE** or modify any evidence, even if it is distressing.
- ✗ Avoid confronting or contacting the perpetrator directly.
- ✗ Consult legal or support entities before taking public action.

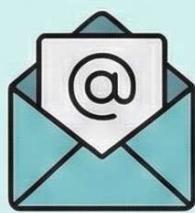
REPORTING TO AUTHORITIES

Secure processes for filing complaints and escalating cases for NCII and CSAM.



1. Law Enforcement Reporting

- National Cyber Crime Reporting Portal:
<https://cybercrime.gov.in>
- Thuna Portal / Pol App:
<https://thuna.keralapolice.gov.in/>
- Visit Nearest Cyber Crime Police Station in person.



2. Escalation Emails for Faster Investigation

- SP Cyber Operations:
spcyberops.pol@kerala.gov.in
- ADGP Cyber Operations:
adgpcyberops.pol@kerala.gov.in
- Contact District Police Chief & DIG for further attention.



3. Priority & Circulation Warning

- **Be Aware:** Content may circulate on Telegram, dark web forums.
- National portal utilizes Hash-based takedown via Sahyog portal to prevent further circulation.
- Mark as 'High Priority' during reporting for urgent action.



Important Notes

- Keep all complaint acknowledgment numbers safe.
- Preserve digital evidence before reporting.
- Maintain communication records with authorities.
- Follow up regularly for updates.

CONTENT REMOVAL & TRUSTED PLATFORMS

Empowering survivors to report and remove non-consensual content and CSAM.



General Support & Helplines



- <https://revengepornhelpline.org.uk/> ↗
- <https://aarambhindia.org/> ↗

AUTOMATED TAKEDOWN TOOLS



- Adults (18+):
<https://stopncii.org/> ↗



- Minors (<18):
<https://takeitdown.ncmec.org/>

Social Media & CSAM Reporting



- <https://report.cybertip.org/> ↗
- <https://report.iwf.org.uk/in> ↗
- <https://meldpunt.offlimits.nl/> ↗

IMPORTANT NOTE



- Platforms store **only hash values** of the content for removal purposes. Your original **content NEVER leaves your device**, ensuring privacy and security during the reporting process.

KERALA POLICE, CYBERDOME & CCSE UNIT

Key Contact Information & Resources for
Cyber Safety and Support



CCSE Unit (Counter Child Sexual Exploitation)

- • ccse.pol@kerala.gov.in



Support & Resources

- **One Stop Centres:** Available in all districts across Kerala for integrated support.
- **MeitY NCII SOP PDF:** Download Standard Operating Procedure for Non-Consensual Intimate Imagery.
<https://www.meity.gov.in/static/uploads/2025/11/a2c9500ef5f8b62a43bfc68747de592d.pdf>



Cyberdome Units (Cyber Centres of Excellence)

- **Cyberdome TVPM (Trivandrum):** cyberdome.pol@kerala.gov.in
- **Cyberdome Kochi (Ernakulam):** cyberdomeekm.pol@kerala.gov.in
- **Cyberdome KKD (Kozhikode):** cyberdomekkd.pol@kerala.gov.in



IMPORTANT WARNING

- Only family members or legal representatives can take action on behalf of the survivor.
- Sharing, distributing, or possessing CSAM (Child Sexual Abuse Material) is a punishable offense under the POCSO Act & IT Act.

NGO SUPPORT & COUNSELLING

Compassionate care, legal guidance, and emotional support resources.



Emergency Support



Trauma Counselling



Legal Guidance



Parihar (Bengaluru)

✉️ pariharfcc.vsv@gmail.com
📞 080-22943225



Breakthrough

🌐 <https://inbreakthrough.org/>



CSR (Centre for Social Research)

🌐 <https://www.csrintdia.org/>



RATI Foundation

🌐 <https://ratifoundation.org/>



Red Dot Foundation (Safecity)

🌐 <https://safecity.in/>



Responsible Netism

🌐 <https://responsiblenetism.org/>



Social Media Matters



🌐 <https://socialmediamatters.in/>

DIGITAL HYGIENE & PRIVACY SAFEGUARDS

Essential checklist for securing your online presence and data.



Change passwords (email, social media, cloud accounts). Use strong, unique passwords.



Enable two-factor authentication (2FA) on all sensitive accounts for an extra security layer.



Audit devices, backups, and app permissions. Review connected devices and data access.



Check for spyware or unauthorized access. Run regular security scans and monitor account activity.



Remove public photos; set accounts to private. Review and adjust privacy settings on all platforms.

TRAUMA & PSYCHOLOGICAL SUPPORT

Guidance for healing, resilience, and mental well-being.

Professional Support & Counselling



- 就医 Use One Stop Centres (OSC), NGOs, or private counselors for trauma-informed care.
- 心理 Access confidential and specialized psychological support services. ❤️

Digital Well-being & Self-Care



- 避开 Avoid over-monitoring content online; take breaks from digital platforms.
- 实践 Practice mindfulness and engaging in offline activities to reduce digital stress. 📖

Community & Peer Support



- 加入 Join support groups to share experiences, reduce stress, and gain legal guidance. 🧑‍🤝‍🧑
- 连接 Connect with others who understand for emotional empowerment and collective strength. ⭐

Remember, healing is a journey.
You are not alone, and help is available.

EXPLICIT DO'S & DON'TS

Critical guidelines for handling non-consensual content and CSAM cases.



Do:

- ✓ Preserve evidence, report immediately.
- ✓ Involve trusted family, guardian, or lawyer.
- ✓ Contact NGOs or cybercrime units for guidance.



Don't:

- ✗ Download, store, forward, share images/videos.
- ✗ Post publicly about your case.
- ✗ Negotiate takedown privately.
- ✗ Act alone — legal/family support is mandatory.



Remember: Your safety and legal protection are paramount. Seek professional help immediately.

HARD TRUTHS

Understanding the limitations of content removal
in private and encrypted channels.



CONTENT CIRCULATING IN PRIVATE/ENCRYPTED CHANNELS

Cannot be removed.

Public search engines cannot index or remove content from closed, encrypted groups (e.g., Telegram) or dark web forums.

REMOVAL DEPENDS ON:



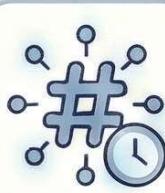
PLATFORM MODERATION

- Each platform has its own terms of service and moderation policies.
- Content removal is subject to the platform's review and enforcement actions.
- Private channels often have limited moderation compared to public platforms.



LAW ENFORCEMENT INVESTIGATION

- Formal complaints to law enforcement are crucial.
- Authorities can issue takedown notices and track perpetrators.
- Investigation timelines vary and depend on jurisdiction and evidence.



HASH-BASED BLOCKING OVER TIME

- Unique digital fingerprints (hashes) of content are used for identification.
- Platforms can use hashes to prevent re-uploading and block distribution.
- This process is proactive but requires the content to be previously identified and hashed.



While immediate removal may be challenging in private spaces, combining reporting, law enforcement involvement, and technological solutions increases the chances of effective action and prevention over time.

High Court Intervention (Article 226 Writ Petition)

Legal process and remedies for expedited removal of non-consensual content and CSAM through a writ petition under Article 226 of the Constitution of India.



1. File Writ Petition under Article 226

- Engage a qualified advocate to file a petition before the High Court invoking its writ jurisdiction for protection of fundamental rights.



2. Request In-Camera Hearing

- Pray for private proceedings to protect the survivor's identity and dignity, excluding public and media presence.

⚠ Important: Discretion of the Hon'ble Court.



3. Sealed Records / Confidential Annexures

- Submit sensitive information (URLs, evidence, personal details) in a sealed cover, not accessible to the public or media.
- Request for Non-disclosure / Gag Orders against platform intermediaries and media.



4. Pray for Specific Remedies:

- Police / Cyber Cell Investigation:** Direction for expedited FIR registration and dedicated investigation.
- Platform Takedown & Hash Blocking:** Immediate removal of content and hashing to prevent re-upload.
- Search Engine De-indexing:** Removal of search results leading to the content.
- Blocking Orders to MeitY:** Direction to the Ministry of Electronics and Information Technology for blocking content at the ISP level.
- Time-bound Compliance Reports:** Direction for platforms and authorities to file compliance reports within a specified timeframe.



5. Ongoing Monitoring & Compliance

- The Court may monitor the progress and ensure strict adherence to its orders by all parties.



We are only providing information from publicly available online resources. This is not legal advice. Please consult a qualified lawyer or advocate for accurate guidance specific to your situation.

EMERGENCY HELPLINES & CONCLUSION

National Cyber Crime Helpline



1930

For reporting all types of cybercrime, including NCII.
Available 24/7 across India.

Childline India



1098

A 24-hour, free, emergency phone service for children in distress.



Remember the **Standard Operating Procedure (SOP):**
Ensure Safety → Preserve Evidence → Report to Authorities → Seek Support.

You are not alone in this journey. Utilize these resources, lean on your trusted support system, and prioritize your healing. Justice and recovery are possible.

Stay Safe. Stay Informed.