“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.

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.

Reminder: You are not alone; support is available.

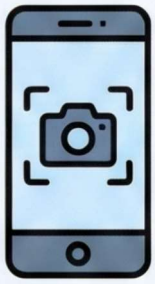
3. ACCESS PROFESSIONAL GUIDANCE

- 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.

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.

KERALA POLICE – CYBER CRIME SUPPORT CONTACTS

Official Cyber Cell and Cyber Crime Police Station Contact Details

CYBER CELL CONTACT DETAILS

Sr No	Designation	Office Contact	Mobile	Email
1	Cyber Cell Kollam City	0474-2744165	9497960680	cbrcelklm.pol@kerala.gov.in
2	Cyber Cell Thrissur City	-	9497962836	cbrceltsr.pol@kerala.gov.in
3	Cyber Cell Kasaragode	04994-257800	9497976013	cbrcelksd.pol@kerala.gov.in
4	Cyber Cell Kollam Rural	0474-2450180	9497980211	cybcelklmrl.pol@kerala.gov.in
5	Cyber Cell Thrissur Rural	-	9497976006	cybceltsrrl.pol@kerala.gov.in
6	Cyber Cell Pathanamthitta	0468-2327914	9497976001	cbrcelpta.pol@kerala.gov.in
7	Cyber Cell Palakkad	-	9497976037, 9497976038	cbrcelpkd.pol@kerala.gov.in
8	Cyber Cell Alappuzha	0477-2230804	9497981288, 9497976000	cybrcelalpy.pol@kerala.gov.in
9	Cyber Cell Malappuram	-	9497976008	cbrcelmpm.pol@kerala.gov.in
10	Cyber Cell Kottayam	0481-2561304	9497976002	cbrcelktm.pol@kerala.gov.in
11	Cyber Cell Kozhikkode City	-	9497976009	cbrcelkkd.pol@kerala.gov.in
12	Hitech Cell PHQ	0471-2721547	9497900468	hitechcell.pol@kerala.gov.in
13	Cyber Cell Idukki	-	9497976003	cbrcelidk.pol@kerala.gov.in
14	Cyber Cell Kozhikkode Rural	-	9497976043	cybcelkkdrl.pol@kerala.gov.in
15	Cyber Cell Thiruvananthapuram City	0471-2329107	9497975998	cbrceltvm.pol@kerala.gov.in
16	Cyber Cell Kochi City	0484-4019664	9497976004	cbrcelekm.pol@kerala.gov.in
17	Cyber Cell Wayanad	-	9497976011	cbrcelwynd.pol@kerala.gov.in
18	Cyber Cell Thiruvananthapuram Rural	0471-2303066	-	cybceltvmrl.pol@kerala.gov.in
19	Cyber Cell Ernakulam Rural	0484-2630238	9497976005	cybcelekmrl.pol@kerala.gov.in
20	Cyber Cell Kannur	0497-2763332	9497976012	cbrcelknr.pol@kerala.gov.in

CYBER CRIME POLICE STATION CONTACT DETAILS

Sr No	Designation	Office Contact	Mobile	Email
1	Cyber Crime Police Station Thiruvananthapuram City	0471-2322090	-	cyberps.pol@kerala.gov.in
2	Cyber Crime PS Thiruvananthapuram Rural	0471-2301070	9497960343	cyberpstvmrl.pol@kerala.gov.in
3	Cyber Crime Police Station Kollam City	-	9497960680	cyberpsklm.pol@kerala.gov.in
4	Cyber Crime Police Station Kollam Rural	-	9497980211	cyberpsklmrl.pol@kerala.gov.in
5	Cyber Crime Police Station Pathanamthitta	-	9497961078	cyberpspta.pol@kerala.gov.in
6	Cyber Crime Police Station Alappuzha	0477-2990121	9497981288	cyberpsalpy.pol@kerala.gov.in
7	Cyber Crime Police Station Kottayam	-	9497976002	cyberpsktm.pol@kerala.gov.in
8	Cyber Crime Police Station Idukki	04862-2232319	9497976003	cyberpsidk.pol@kerala.gov.in
9	Cyber Crime Police Station Ernakulam City	0484-2956900	9497947267	cyberpskochi.pol@kerala.gov.in
10	Cyber Crime PS Ernakulam Rural	0484-2955006	9497960578	cyberpsekmrl.pol@kerala.gov.in
11	Cyber Crime Police Station Thrissur City	0487-2952050	9497947269	cyberpstsr.pol@kerala.gov.in
12	Cyber Crime Police Station Thrissur Rural	-	9497919293	cyberpstsrrl.pol@kerala.gov.in
13	Cyber Crime Police Station Palakkad	0491-2536090	9497919536	cyberpspkd.pol@kerala.gov.in
14	Cyber Crime Police Station Malappuram	0483-2735777	9497934293	cyberpsmpm.pol@kerala.gov.in
15	Cyber Crime Police Station Kozhikode City	0495-2970400	9497987184	cyberpskkd.pol@kerala.gov.in
16	Cyber Crime Police Station Kozhikode Rural	-	9497976010	cyberpskkdrl.pol@kerala.gov.in
17	Cyber Crime Police Station Wayanad	04936-2205525	9497925225	cyberpswynd.pol@kerala.gov.in
18	Cyber Crime Police Station Kannur City	-	9497976012	cyberpsknr.pol@kerala.gov.in
19	Cyber Crime PS Kasaragod	-	9497976013	cyberpsksd.pol@kerala.gov.in

NCII & CYBERCRIME – CENTRAL LEVEL ESCALATION

Official escalation, DMCA takedown, and safe reporting process

CENTRAL LEVEL ESCALATION (NCRP / I4C)

National Cyber Crime Reporting Portal – Higher Authorities

- **Director (NCRP – I4C-1)**
  Sh. Manish Garg
  Email: dir-i4c1[at]gov[dot]in
- **CEO – I4C**
  Sh. Rajesh Kumar
  Email: ceo-i4c[at]mha[dot]gov[dot]in
- **Deputy Director (NCRP – I4C-1)**
  Sh. Mayank Ghildiyal
  Email: dd-i4c1[at]gov[dot]in

I4C handles monitoring, coordination, and platform takedown. Investigation remains with State Police.

DMCA / NCII TAKEDOWN (ALL PLATFORMS)

Immediate Content Removal – DMCA / NCII

- Report **Non-Consensual Intimate Images (NCII)** on every platform
- Bundle multiple URLs platform-wise

- **Google** – Report Nudity / Graphic Sexual Content
  https://support.google.com/legal/contact/lr_idmec?sjid=15428026171101035256-NC
- **X (Twitter)** – Safety & Sensitive Content
  https://help.x.com/en/forms/safety-and-sensitive-content/cse

ESCALATION VIA PG PORTAL (LAST OPTION)

Public Grievance Portal (pgportal.gov.in)

1. **Ministry**: Department of Home Affairs
2. **Main Category**: Crime Related – Cyber Cell

- Keep complaint extremely brief
- **Do NOT** upload images, videos, or NCII content
- Mention only:
  – NCRP Acknowledgement Number
  – Request for urgent escalation

Not recommended unless all other escalation methods fail. Do not expect immediate resolution.

IMPORTANT SAFETY NOTES

- Never upload NCII images or videos anywhere
- Preserve evidence (URLs, screenshots, acknowledgement numbers)
- Avoid direct confrontation with perpetrators
- Maintain records of all communications

Aparajitha is Online

Ensuring safe, confidential, and rapid police response to online harassment.

WHY THIS MATTERS

Why many cases go unreported

- Social pressure and fear of stigma
- Offender often known (friend / relative)
- Blackmail and emotional pressure
- Lack of confidence approaching police

A sensitive and technically robust response system is essential.

PROCESS FLOW

How the System Works

1. Complaint received via exclusive email
2. Forwarded to concerned police station
3. Enquiry to identify and locate offender
4. Support from Cyber Cell, District Cyber Cell, Hi-Tech Cell, Cyber Dome
5. Victim informed
6. Legal action initiated by SHO if required

ROLE & RESPONSIBILITY

Who Handles Complaints

- SP Women Cell
- State-level and Police Station-level grievance redressal
- Trained cyber-savvy WCPO / WSCPO officers

CONFIDENTIALITY & SUPPORT

Key Assurances to Victims

- Utmost confidentiality of victim and family
- No victim shaming
- Protection from further harassment
- Empathy, tact, and cyber awareness as core principles

Report Online Harassment

aparajitha.pol@kerala.gov.in

CYBER OPERATIONS CONTACT DETAILS

IGP Cyber Operations	SP Cyber Operations
Office: 0471-2726522	**Office:** 0471-2315965
Mobile: 94979 97997	**Mobile:** 94979 96923
Email: adgpcyberops.pol@kerala.gov.in	**Email:** spcyberops.pol@kerala.gov.in

- **DySP Cyber Operations:** dyspcyberops.pol@kerala.gov.in
- **Public Outreach Group:** k4cict.pol@kerala.gov.in
- **Cyber Fraud & Social Media Group:** cyberops-fsm.pol@kerala.gov.in
- **Cyber Security & Advanced Cyber Crime Group:** cyberops-sec.pol@kerala.gov.in
- **Cyber Dome:** cyberdome.pol@kerala.gov.in
- **Training & Capacity Building Wing:** cyberops-trg.pol@kerala.gov.in
- **Analysis Wing:** cyberops-raw.pol@kerala.gov.in

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

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

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

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.csrindia.org/

RATI Foundation

https://ratifoundation.org/

Red Dot Foundation (Safecity)

https://safecity.in/

Responsible Netism

https://responsiblenetism.org/

Social Media Matters

https://socialmediamatters.in/

Note: These resources provide confidential support. Contact them for assistance.

DIGITAL HYGIENE & PRIVACY SAFEGUARDS

Essential checklist for securing your online presence and data.

- [x] Change passwords (email, social media, cloud accounts). Use strong, unique passwords.
- [x] Enable two-factor authentication (2FA) on all sensitive accounts for an extra security layer.
- [x] Audit devices, backups, and app permissions. Review connected devices and data access.
- [x] Check for spyware or unauthorized access. Run regular security scans and monitor account activity.
- [x] 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

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

Digital Well-being & Self-Care

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

Community & Peer Support

- Join support groups to share experiences, reduce stress, and gain legal guidance.
- 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.

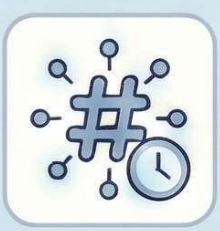
REMOVAL DEPENDS ON:

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

- Request the court to seal records containing sensitive information (such as evidence or personal details) to restrict public access.
- 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.

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.