unicef
for every child

D-Safe

ENDING ONLINE ABUSE AND VIOLENCE AGAINST CHILDREN

A CASE STUDY BASED GUIDANCE DOCUMENT FOR PARENTS

CaP
CHILDREN AND POLICE
STATE RESOURCE CENTRE
A CaP for CARE & PROTECTION

unicef
for every child

D-Safe

ENDING ONLINE ABUSE AND VIOLENCE AGAINST CHILDREN

A CASE STUDY BASED GUIDANCE DOCUMENT FOR PARENTS

About the Booklet

This booklet is aimed at equipping several parents and teachers and thereby adolescents, to promote the safe use of the internet and to protect themselves and others from online abuse and violence.

This booklet discusses certain scenarios when children are prone to be victimised in the cyber world, adapted from real recorded cases dealt with by Kerala Police, by hiding their identity. Each scenario is analysed holistically, encompassing the technical, legal, and psycho-social aspects.

This booklet also consists of contact information regarding various Governmental and Non- Governmental agencies which help in redressing the grievances.

Published by

CaP
CHILDREN AND POLICE
STATE RESOURCE CENTRE
A CaP for CARE & PROTECTION

unicef
for every child

D-Safe

ENDING ONLINE ABUSE AND VIOLENCE AGAINST CHILDREN

A CASE STUDY BASED GUIDANCE DOCUMENT FOR PARENTS

Contributors

Mr. Pious Mathew (Advocate, Former PP POCSO Act cases, Thrissur)

Dr. Smitha Ramdas (Addl. Professor, Dept. of Psychiatry, GMCH, Thrissur)

Dr. Baspin (Member, CWC) Thrissur

Mr. Prasreen Kunnampilly (State Coordinator, Bachpan Bachao Andolan)

Mr. Shijin Chandran (Cyber Forensics Consultant, KEPA)

Dr. Jayesh K Joseph (Criminologist, KEPA)

Dr. P. Sachidanandan (HOD, Dept, of Forensic Sciences, KEPA)

Mr. E. P. Ramdas (Inspector of Police, KEPA)

Ms. Soumya Mohan C (HOD, Dept. of Behavioural Sciences, KEPA).

Ms. Rima Joseph (Clinical Psychologist, CAP House-SRC,Thiruvananthapuram)

Artist Nandan Pillai (Chairman, Orgpeople India Foundation)

Cyber Cell, Thrissur

Cyber-Forensics Lab and R&P Wing, KEPA

Published by

CHILDREN AND POLICE
STATE RESOURCE CENTRE
A CAP for CARE & PROTECTION

unicef
for every child

D-Safe

ENDING ONLINE ABUSE AND VIOLENCE AGAINST CHILDREN

A CASE STUDY BASED GUIDANCE DOCUMENT FOR PARENTS

Foreword

Kerala Police is nationally renowned for consistently providing quality police services to citizens. Numerous national surveys, including the recent one by the Indian Police Foundation, have proved this fact beyond doubt. Apart from providing quality services, Kerala Police has always been in the forefront of the fight against cybercrimes.

Kerala Police is one of the few police forces around the globe to think about a dedicated wing to coordinate cyber-based investigations and provide services of technical experts. It has introduced many initiatives like hackathons for police action on the Dark Web and Operation P-hunt to track sharing of paedophile pornographic contents. Cyberdome is another visionary initiative of Kerala Police to meet the long term security challenges posed by the modern world. The Cyber Crime Police Stations investigate serious and complex Cyber-crimes, which require high technical and Cyber forensic expertise.

We understand that the children are the most vulnerable in the present day world. They are surrounded with challenges that their previous generations could not even think of. Hence, care, protection and security of children are in the priority list of Kerala Police. Student Police Cadets Program, Child Friendly Police Stations, Hope Project, 'Chiri' are some of the impactful child centred initiatives of Kerala Police. A state level unit called Children and Police (CAP) House has been established under the recently formed Social Policing Division (SPD) of Kerala Police for better Coordination and implementation of these programs.

I am extremely happy that Social Policing Directorate in partnership with UNICEF has developed a manual called 'D-Safe' to prevent child abuse and violence against children, in the digital space. This manual based on real time case studies, will certainly help to build the capacity of parents and teachers to prevent online crimes against children and effectively respond to such atrocities in the virtual world. I sincerely congratulate the technological, legal and mental health experts who have immensely contributed to prepare this manual.

Anil Kant IPS
DGP & State Police Chief

unicef
for every child

D-Safe
ENDING ONLINE ABUSE AND VIOLENCE AGAINST CHILDREN

A CASE STUDY BASED GUIDANCE DOCUMENT FOR PARENTS

Foreword

Digital technology is synonymous with the modern times that we live in. Love it or detest it, technology affects everything that we do today. It won't be exaggerating to say that no human being of our times is free to escape from the clasps of technology. From the living rooms to the remotest corner of our kitchen, the presence of technology can be felt. The way we communicate, carry out our daily chores, learn, think, anything and everything is influenced by technology.

Technological revolutions, for sure have helped us make strides that our ancestors could not even dream of. However, it has also resulted in a huge digital divide between elders and the youth. Children, by default, are the natives of the digital world, whereas elders are the immigrants of the virtual world. The Covid-19 pandemic has immensely widened the digital gap between the children of the 21st century and the elders. Prior to the pandemic, parents and teachers used to take necessary measures to restrict the screen time of children, whereas, in the light of the pandemic, we now encourage them to be online for attending their classes from home. With the forced social isolation, they also find solace in the digital world to connect with their friends, play online games and use social media. For many children, exposure to the physical world only happens when they move out of their screen to eat or sleep!

National Centre for Missing and Exploited Children (NCMEC) indicates a 106% increase in reports of suspected child sexual exploitation. This signposts the fact that the anti-social elements working for luring children to their clutches have also mostly shifted their operations to the digital world. As a consequence, susceptible children easily fall prey resulting in online abuse and violence. The situation has become so gruesome that online abuse and violence should not be the concern of law enforcement agencies alone anymore. Everyone should now be prepared to be the First Responders in such circumstances.

In this context, the Social Policing Directorate of Kerala Police has conceived a unique capacity development program based on a scientifically drafted manual based on real-time pieces of evidence. This manual titled 'D-Safe' is developed by a team of carefully selected technological, legal, and psychological experts committed to fighting the social evil - online abuse, and violence against children. This manual would not have materialised without the partnership of UNICEF and support of Kerala Police Academy (KEPA). Based on this manual built on actual case studies, a state-level army of trainers will be created to lead capacity-building programs for enabling teachers and parents. By December 2022, we plan to enable every parent and teacher of Kerala, to become a first responder in instances of online abuse and violence.

P.Vijayan IPS
Inspector General of Police

INDEX

THE CONTENT OF THE BOOK INCLUDE:

Scenarios and needed interventions related to :

Scenario 1

Cyberbullying

Revathy is a 9th Standard girl having accounts in Social Media platforms though not active. Once she received a message from an unknown lady's Instagram account to which she responded.

She was slowly groomed into a friendly relationship and they exchanged photos. The lady on the other end figured the girl's interest in the film field, started to flatter her comparing her to some film actresses, and suggested posting photos in certain poses and attire to which the girl responded positively.

After one week, this lady sent the girl her morphed naked photos and threatened the girl that if she won't send some real naked photos she would post these on social media.

The desperate girl had to do exactly what the lady instructed. On receiving those photos, the lady started to intimidate and demand more such photos irrespective of her disinterest.

The girl became upset and depressed. Observing this her parents took the help of a counsellor and eventually, the entire event was disclosed.

The investigation by the Police revealed that the person on the other end was a man in disguise.

Technical Aspects

Actions to be taken

- Collect the Instagram ID of the lady's account along with the date and time of the incident by taking screenshots of her profile page.
- Report the crime in the Online Cyber Crime Reporting Portal or nearest Police Station.
- Report the profile to the Instagram officials by taping the "report" option.

Preventive Measures

- Identify the person in the real world before accepting friend requests or follow requests from unknown people.
- Do not chat with unknown people on social media platforms.
- Make your account private and choose who can see your posts.
- Make all your posts and photos visible to friends only
- Do not share user credentials with anyone.

Legal Aspects

This crime includes cyber grooming, bullying, intimidation, morphing, the transmission of child pornography, etc. These crimes are punishable under the POCSO Act, IPC, and IT Act for a maximum period of 7 years. If the victim belongs to SC/ST or physically/mentally challenged category then the corresponding Acts will be applicable and punishment will be more. Since the accused person is a Child in conflict with the law, these offences shall be dealt with under the provisions of the JJ Act. Such offences need to be reported to the Police at the earliest.

Sections of law applicable :

- Sec.12 r/w 11, 14 r/w 13, and 15 of the POCSO Act
- Sec.354A, 499, 354D, 503, 506, 509 of the IPC
- Sec.66D, 66E, 67, 67B of the IT Act

Psycho-Socio Aspects

How to respond?

- Be calm, be with the girl and be careful not to blame her.
- Assure her that the help is available.
- Encourage her to take action legally for her negative experience.
- Accept the fact that worrying is normal and help her to rebuild trust.
- Take her to a therapist if the bullying was traumatic for her.
- Convince her to seek support from parents and teachers whenever she becomes uncomfortable online.
- After the acute crisis, teach her about the safe use of technology and assertiveness skills - how to say "no".

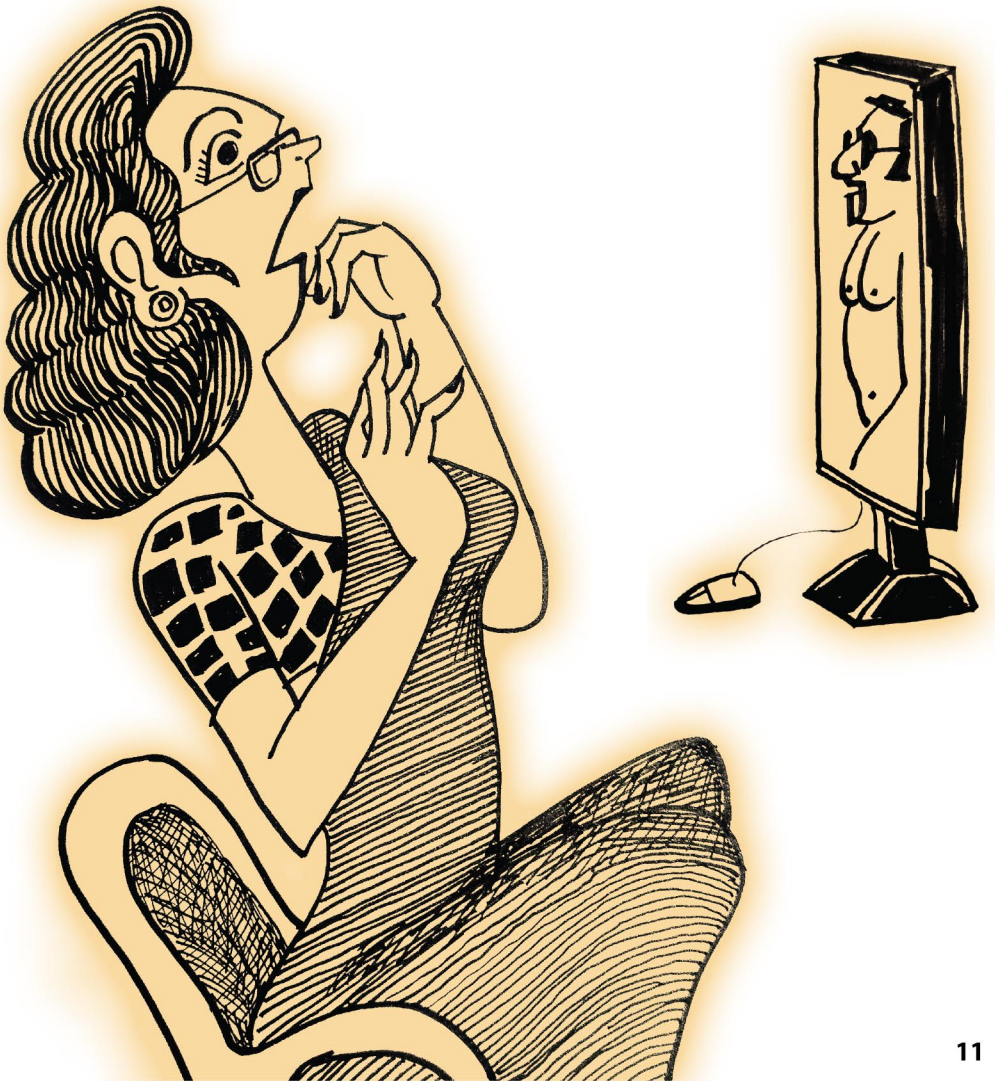
Scenario 2

Online class intrusion

During the online class of 4th standard students, an unidentified person appeared nude and displayed some obscene photos in the live class. He was wearing a helmet to hide his face.

The teacher removed the intruder but he joined again using another account and repeated the same. With no other options left, the teacher ended the class. These kinds of online class intrusion incidents are becoming very common.

While the schools and colleges are conducting online classes, teachers and students are troubled by hackers who sneak into online classrooms, often displaying vulgar content on the screens.



Technical Aspects

Actions to be taken

- Take screenshots of the mail ID, display name and profile picture of the offender.
- Take screen recordings of the abusive content shared in the class.
- Save the meeting ID, date and time of the incident.
- Collect all mail IDs and mobile numbers of the students who attended the class.
- Report the account to Google officials by taping "report a problem" under three dots.
- Report this crime in the Online Cyber Crime Reporting Portal or nearest Police Station.

Preventive Measures

- Share the meeting links only to the emails of the students and not through WhatsApp groups.
- Do not press "admit all" participants before starting the class.
- Accept the participants individually only after verification.
- Do not share the entire screen of the device while taking classes. Share only the presentation window with the students.

Legal Aspects

This crime includes sexual harassment, the transmission of pornographic material to children, etc. These crimes are punishable under the POCSO Act, IPC, and IT Act for a maximum period of 7 years. Such offences need to be reported to the Police at the earliest.

Sections of law applicable :

- Sec.12 r/w 11, 14 r/w 13, and 15 (if applicable) of the POCSO Act
- Sec.67, 67A of the IT Act
- Sec.292, 354, 509 of the IPC
- Sec.119 of the KP Act

Psycho-Socio Aspects

How to respond?

- Make them understand that certain things are not under our control and it is natural even if they feel bad about the incident.
- Do not discourage children when she/he enquires about the human body and nudity.
- Educate them about the human body age-appropriately.
- Find out if anyone is having recurrent thoughts about the incident. If so seek the support of a mental health professional.
- Keep track of all the students in the class and help mutually.
- Train basics of assertiveness skills and teach them the appropriate and inappropriate behaviours about personal space.
- Use this opportunity to educate children about online safety, internet etiquette and encourage open dialogue with the students.

Movie Piracy

Rajesh runs a Mobile Phone service - Internet Café Shop. His 15-year-old son, Pranav, used to help his father in the shop after his class hours.

He was deceitfully making some pocket money by copying and selling some newly released films to some customers without the knowledge of his father.

One day the Anti-Piracy Cell raided the shop and a case was registered against his father for piracy.

Technical Aspects

Actions to be taken

- Report this crime in the Online Cyber Crime Reporting Portal or at the nearest police station.

Preventive Measures

- Never download or share copyright-protected videos and movies published on online platforms.
- If someone downloads or shares such content, report it to the concerned.
  Conduct awareness classes for the students about the consequences of such actions.

Legal Aspects

This is a clear case of piracy. Though it was done by the 15-year-old son of the shop owner without the knowledge of his father, the father will be held liable for prosecution. The offence is punishable by up to 3 years imprisonment and a fine.

Sections of law applicable :

- Sec.63 of the Copyright Act, 1957
- Sec.7 of the Cinematographic Act

Psycho-Socio Aspects

How to respond?

- Do not blame him right away even though he needs to be intervened.
- Make him witness all the disciplinary procedures going on as the consequences of his behaviour.
- Make him narrate what he understood.
- Make him narrate how this happened and what was his contribution.
- Make him say by himself how he should be careful about this ill-handling of situations. Also, ensure that the child's mental health is not adversely affected.
- In case the child is not having any remorse or concerns regarding the event, behavioural management needs to be carried out with the help of a mental health professional.
- Do not isolate him from the family.
- Use this opportunity to educate him about online safety and internet etiquette.
- Continue mental health interventions as the situation and his condition demand.
- Support and educate the family about the safe use of the internet.

Scenario 4

Online gaming & Account takeover

Ananthan, who studies in 7th standard, plays online games regularly. He uses his father's Facebook account to log into the gaming application. As he reached higher levels of the game, an unknown person approached him and offered money to exchange the gaming account with user credentials. He agreed and shared his ID and password.

Later the person denied the payment that he offered and subsequently changed the login ID and password. As a result, Ananthan was not able to retrieve the account. The stranger demanded money when Ananthan asked for the credentials back. Somehow he managed to send a little money but the person kept demanding more money.

Ananthan did not disclose this matter to anyone. As the offender stopped getting money, he posted some obscene content through the Facebook account, and only then did his father come to know about the matter. Subsequently, they went to the police station and filed a complaint.

Online games are making our kids addicted to them. Most of the children do not have bank accounts. However, they frequently use their parents' accounts for doing online transactions for gaming, shopping, etc. Criminals use several fraudulent tactics to steal money from the accounts.

Technical Aspects

Actions to be taken

- Take the screenshot and URL of the obscene content shared on Facebook.
- Collect all available details (screenshots, mobile number, bank account number, etc.) of the account to which the game user credentials were shared.
- Report the profile as 'hacked' and request Facebook for access to the account.
- Report this crime in the Online Cyber Crime Reporting Portal or nearest Police Station.
- After the recovery of the Facebook account, change the password, remove all other verified devices and applications and enable two-step verification.
- Download "Your Information" from the account and share it with the police for investi-

Preventive Measures

- Never use parents' mobile phones for playing games since the social media accounts are signed in by default.
- Use two-factor authentication on Facebook.
- Sign out from social media accounts while giving mobile phones to the children for studying or gaming.
- Do not share passwords of the e-wallets and online banking with children.
- Do not save credit/debit card details on the device.
- Use separate devices for banking purposes if possible.

Legal Aspects

This is a case of cheating and hacking. The person also published obscene material. These acts are punishable under the IT Act and the IPC for a maximum term of 7 years and fine/compensation.

Sections of law applicable :

- Sec.43, 66, 66C, 66D, 67A of the Information Technology Act, 2000
- Sec. 420 of the IPC

Psycho-Socio Aspects

How to respond?

- Do not blame him right away even though he needs to be intervened.
- Make him witness all the disciplinary procedures going on as the consequences of his behaviour.
- Make him narrate what he understood.
- Make him narrate how this happened and what was his contribution.
- Make him say by himself how he should be careful about this ill-handling of situations. Also, ensure that the child's mental health is not adversely affected.
- In case the child is not having any remorse or concerns regarding the event, behavioural management needs to be carried out with the help of a mental health professional.
- Do not isolate him from the family.
- Use this opportunity to educate him about online safety and internet etiquette.
- Continue mental health interventions as the situation and his condition demand.
- Support and educate the family about the safe use of the internet.

Scenario 5

Online defamation

Aromal uses his father's phone for attending his online classes. He was an admin of the WhatsApp group comprising his classmates. He regularly updates his WhatsApp status posts.

One day the boy posted content that was defamatory to the government. His father being a government employee had to face the consequences including disciplinary action.

Technical Aspects

Preventive Measures

- Use biometric locks in social media applications.
- Educate children about the consequences of sharing fake, defamatory, and other objectionable material.

Legal Aspects

Sharing/publishing defamatory content against a person/government and propagating fake news are against rules.

Sections of law applicable:

- Sec.499, 500 of the IPC along with appropriate disciplinary proceedings.

Psycho-Socio Aspects

How to respond?

- Don't be prejudiced. Support the child and family if they are distressed.
- Encourage healthy discussions at home at all levels.
- Use this opportunity to educate him about online safety and internet etiquette.
- Seek the help of a mental health professional as and when required.
- Support and educate the family about the safe use of the internet.

Scenario 6

Online nudity

Sai, studying in 8th standard, received a WhatsApp video call from an unknown number. He curiously attended the call. On the other end of the call a naked woman appeared. The boy was shocked and instantly cut the call.

After some time he received a threatening WhatsApp message demanding money with the screen-shot of the boy attending call with the nude lady attached.

Technical Aspects

Immediate Action

- Save the screenshot received from the unknown sender.
- Take a screenshot of the chats and the number from which they came.
- Save the banking details given by the offender.
- Report and block the WhatsApp account from which the call was received.
- Report this crime in the Online Cyber Crime Reporting Portal or the nearest Police Station.

Preventive Measures

- Never take video calls from unknown numbers
- Do not chat with any unknown person that you don't know in the real world.
- Initially cover the camera in case you attend the call.
- Always be aware of the surroundings before you take any video call.
- Do not save the unknown numbers into your contacts which will prevent them from viewing your profile pictures and status updates.

Legal Aspects

Online video calls from unknown numbers targeting students and professionals are becoming common nowadays. Such acts are punishable under the IT Act, the POCSO Act and the IPC for a maximum term of 7 years and a fine.

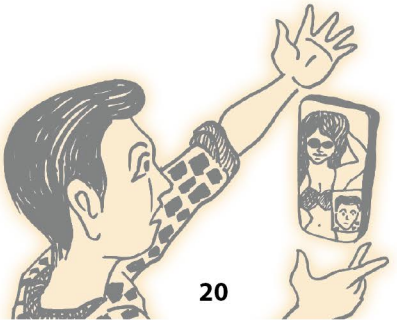
Sections of law applicable :

- Sec.12 r/w 11, 14 r/w 13, and 15 of the POCSO Act
- Sec.67A of the Information Technology Act
- Sec.503 of the IPC

Psycho-Socio Aspects

How to respond?

- Be with the child and help him identify his emotions.
- In case the child is not revealing the actual incident due to shame and fear, give him enough time.
- Encourage him to go for legal actions against the offender and help him go through them.
- Assure him confidence if he constantly worries about the incident.
- Encourage social activities, entertainment and build back the relationship with him.
- Use this opportunity to educate him about online safety and internet etiquette.

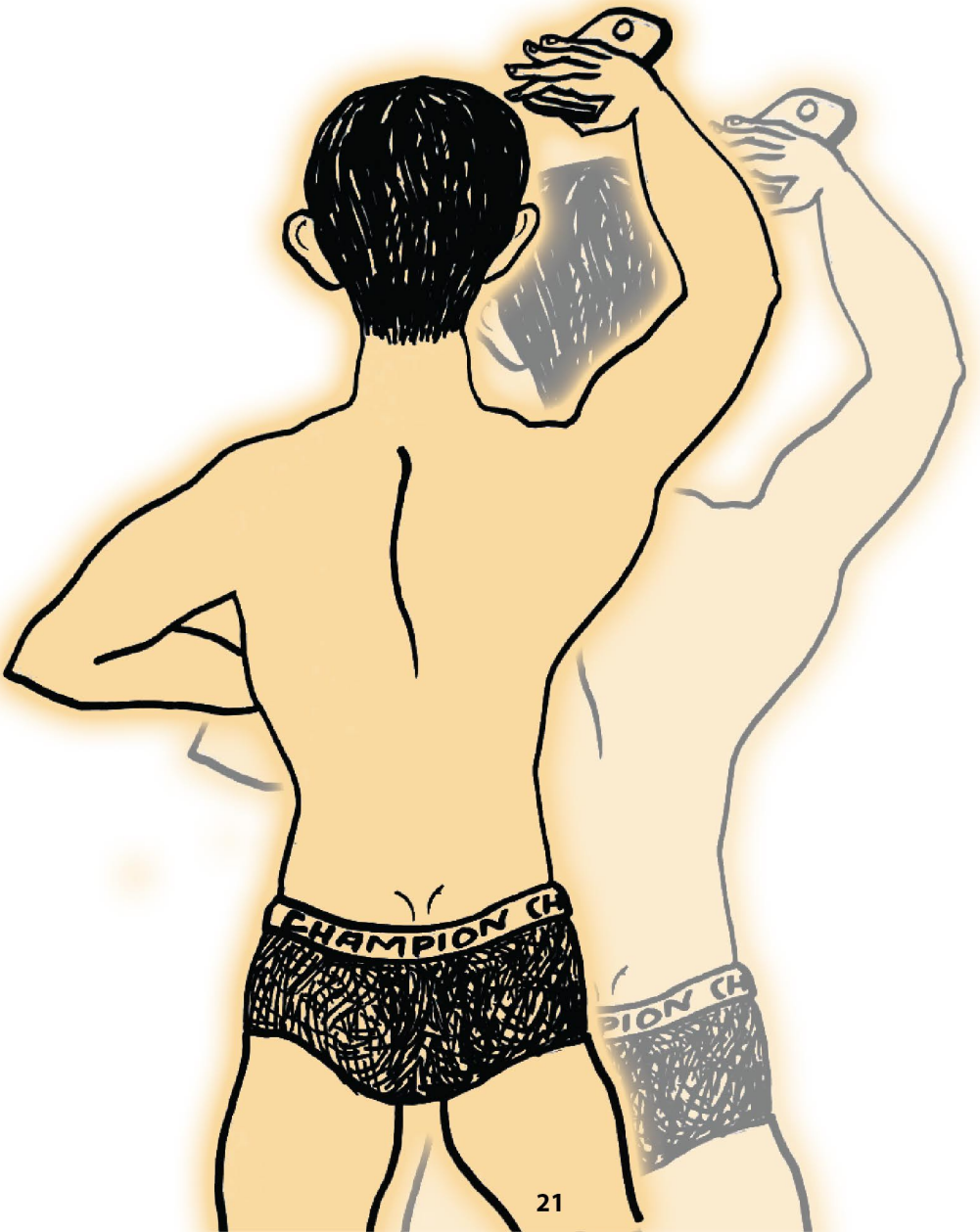


Scenario 7

Child pornography

On receiving the information related to child pornography, Cyber Cell searched a house. It was identified that the accused was a 15- year-old boy. Further investigation revealed that the boy was a member of a WhatsApp group that shares child porn videos.

It was shocking for the investigators that they found some nude photos of his classmates on his mobile phone. On questioning, the boy disclosed that he had to post new photos or videos daily in the group as it was the criterion to continue as a member of the group.



Technical Aspects

Preventive Measures

- Provide awareness to students that searching, viewing, downloading and sharing child pornographic content is a serious offence.
- Verify the internet activities of the child frequently to prevent them from going in the wrong way.
- Exit immediately from groups sharing such materials and report them to the parents/teachers/police.
- Enable Group Privacy settings on your accounts so that nobody can add you to any groups without your permission.

Legal Aspects

Child pornography refers to any content that depicts sexually explicit activities involving a child. According to a recent report by the U.S. National Centre for Missing & Exploited Children (NCMEC), at least 25,000 images of child sexual abuse were uploaded every day from India. This amounts to 12 percentage of the child sexual abuse images circulation globally being generated in India.

Sections of law applicable:

- Sec.15 of the POCSO Act
- Sec.67B of the IT Act

Since the boy is a juvenile in conflict with the law, the case is to be tried before JJB. Also, all the members of the WhatsApp group are liable to be prosecuted under the law. If any one of the members is above 18 years, he is to be tried in a Special court.

Psycho-Socio Aspects

How to respond?

- Be calm and be with the boy.
- Give emotional support.
- Do not blame him.
- Do not get angry or panic.
- Give him space and time for open discussion.
- Support and educate the family about the safe use of the internet, the need to monitor the boy, especially about his online behaviour and how to monitor.
- Help the child to feel valued in the community.
- Help him to be assertive to identify his rights being violated and to respond.
- Encourage him to communicate with parents or trusted people when he becomes uncomfortable online.
- Encourage him to go for legal actions.
- Seek help from mental health professionals.
- Use this opportunity to educate him about online safety and internet etiquette.

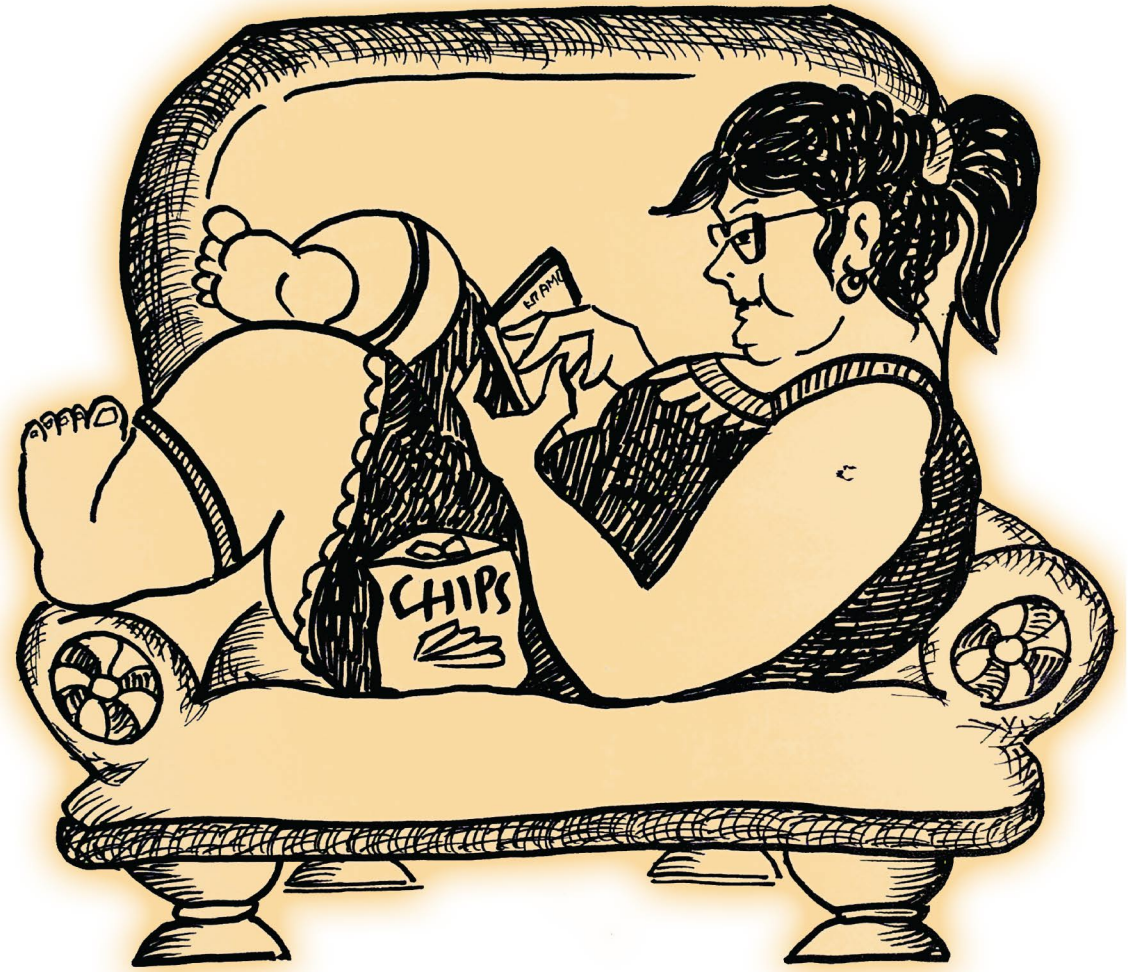
Scenario S8

Mobile addiction

One day a desperate mother approached Cyber Cell to complain about the behaviour changes of her daughter. She was observed to be experiencing sleep deprivation, showing defiance and restlessness and the mother assumed that the problems are related to the over usage of mobile phone.

Investigation revealed the girl was using mobile phone for 18 to 20 hours a day playing some online games which altered her normal behaviour and routine.

Video game addiction, also known as gaming disorder or internet gaming disorder, is generally defined as problematic, compulsive use of video games that results in significant impairment to an individual's ability to function in various life domains over a prolonged period of time.



Technical Aspects

Prevention

- Use parental control applications to restrict device usage.
- Restrict the screen time of the user's device.
- Check the mobile phone to get an idea about the games he played, accounts connected to it, payments he made, etc.

Legal Aspects

If the victim inflicts self-injury or commits suicide as a result of playing the online game, the abettor shall be held liable for punishment under relevant provisions of law.

Psycho-Socio Aspects

How to respond?

- Offer support to the mother and help her to be non-judgemental to her daughter.
- Encourage the mother to seek the help of a mental health professional for her to manage her time spent online, to replace her activities creatively, and to face the withdrawal symptoms adequately.
- Encourage the mother to support her during the treatment without losing patience.
- Educate the mother to communicate with her daughter compassionately.

Scenario 9

Unauthorised access

Neha is a selfie addict. One day she took a selfie for posting on her social media accounts but she didn't post it when she noticed her mother appeared in the selfie changing her dress. Neha even deleted the photo from her device.

After some days, the same photo was seen shared on some social media platforms. On receiving the complaint, Cyber Cell investigated the case. The investigation revealed that earlier the girl had approached an Internet Café near her college for taking printouts of her certificates. She logged in using her mail ID and forgot to log out as she was in a hurry.

The dishonest Internet café owner got access to the Google photos of the girl through her mail ID and uploaded the same on social media.

Technical Aspects

Actions to be taken

- Login to the mail account and remove the unauthorized device.
- Change the password of the account
- Enable two-step verification.
- Take a screenshot/URL of the photo shared on social media platforms.
- Collect the user ID or URL or Mobile Number of the user account along with the date and time in which the photo was posted.
- Report the content to the social media platform concerned.
- Report this crime in the Online Cyber Crime Reporting Portal or nearest Police Station

Preventive Measures

- Always log out from the accounts after logging in from public computers.
- Never share your Gmail username and password with anyone since the same ID is being used for all Google services.
- Disable Google photos if required. Your photos can be seen from anywhere using Google photos if the credentials are known.
- Always opt 'never save' passwords in browsers.
- Use two-factor authentication for mail accounts.
- Be cautious while taking photos containing sexually explicit content or miss usable photos in your phone since they can be recovered at any point in time.

Legal Aspects

The café owner gained unauthorized access to the girl's account and shared obscene content on social media

.

Sections of Law applicable:

- Sec.43, 66, 66B, 66C, 66D, 66E of the Information Technology Act
- Sec.509 of the IPC

Psycho-Socio Aspects

How to respond?

- Be calm and be with the girl.
- Give emotional support.
- Do not blame her.
- Do not get angry or panic.
- Encourage her to go for legal actions.
- Seek help from mental health professionals in case of any difficulty.
- Help the girl build trust in her to approach society normally.

Scenario 10

Online drug sale

Rohith, a 10th standard student, was apprehended by Police as he was found carrying 5 grams of MDMA, a banned drug. Detailed investigation revealed that the boy was a member of a WhatsApp group created by some senior students of his school including some outsiders.

As soon as he joined the group, the admin of the group sent him a small packet of the drug as a welcome gift. After using the drug, he got addicted and wanted more. Since he had no earnings to purchase the drug, he was instructed to deliver certain packets of drugs to some of the regular customers and collect money.

In exchange, he may get a certain quantity of drugs for each supply for his use. Later he was instructed to attract some of his friends into the chain so that he can earn more quantity of drugs.

Technical Aspects

Actions to be taken

- Take screenshots of the chats and the list of members.
- Report and exit the group.
- Report this crime in the Online Cyber Crime Reporting Portal or the nearest Police Station.

Preventive Measures

- Change the 'who can add you to groups' in group privacy settings in WhatsApp as 'my contacts only'.

Legal Aspects

As the boy is a juvenile in conflict with the law, apart from the sections that are applicable against the boy, the other members of the racket will be held liable to be prosecuted u/s 22(c), 27, 29 of the NDPS Act and Sec.370, 109 r/w 34 of the IPC.

Sections of Law applicable to the boy (CCL):

- 22 (c), 27 of the NDPS Act
- Sec.77, 78 of the JJ Act

Psycho-Socio Aspects

How to respond?

- Ensure emotional support to deal with the situation.
- Encourage to seek help from a mental health professional to handle the trauma associated and to overcome the substance addiction.

Scenario 11

Sharing user credentials

Parvathy and Priyanka are 9th standard students. They are very close to each other and share everything including food, clothes, books and even email and social media account credentials.

One day Parvathy noticed that her friend is dating a boy who was an ex-boyfriend of her. On realising that her friend was cheating on her, she couldn't control her anger. She informed Priyanka's parents and this eventually became a very big issue.

Priyanka and her boyfriend decided to give her a reply. Priyanka was having user credentials for Parvathy's email account. She logged into the account from a cybercafé and sent a threatening mail to the Chief Minister. In addition to this, she also sent a mail to some of her classmates and family members containing some obscene pictures of Parvathy which was taken by her ex-boyfriend while they were in a relationship.

On receiving the threatening email, police started the investigation and identified that it has been sent from the email of Parvathy. Police came to her house and examined her. Only then did she come to know that such activities happened through her email ID.

During the investigation, it was understood that her close friend Priyanka had the user credentials of her email account and they were not in a good relationship. On further questioning Priyanka, she confessed that all these acts were done by her and her boyfriend to take revenge on Parvathy.

Technical Aspects

Actions to be taken

- Login to the mail account and remove the unauthorized device.
- Change the password of the account.
- Enable two-step verification.

Preventive Measures

- Never share the user credentials for any online accounts with others.
- Frequently check login activities of your accounts and remove any unauthorised device.

Legal Aspects

Sections of Law applicable :

- Sec.12 r/w 11, 14 r/w 13, 15 of the POCSO Act
- Sec.509, 354A of the IPC
- Sec.66C, 66D, 66E, 67B of the Information Technology Act
- Sec.119(b) of Kerala Police Act

Psycho-Socio Aspects

How to respond?

- Encourage them to seek the help of a mental health professional to address underlying emotional issues and behaviour patterns.
- Encourage parents to deal with the issue with compassion.
- Be supportive of the victim instead of criticizing her.
- Help the teachers to handle the situation effectively.

OTHER ONLINE THREATS AGAINST CHILDREN

KEYLOGGER

It is a program used by cybercriminals to steal the usernames and passwords of a user by recording keystrokes on a computer. Cybercafes are vulnerable to key logger attacks.

CALL/SMS SPOOFING

Call/SMS spoofing happens with the help of spoofing applications developed by hackers with criminal intent to change one's number and voice to impersonate another to defraud the receiver.

RANSOMWARE

Ransomware is a malicious program that encrypts a victim's personal data on a computer. The attacker then demands a ransom from the victim to release the data. This malware generally spreads through emails and free software.

DATING WEBSITES

Online dating websites/Apps create a platform to meet new people, try casual dating, find others with similar interests or finally find your ideal match for a long term relationship. Any private pictures or texts that they send across to the dating companions on such sites can be used to blackmail them.

HACKING

Spy applications are used by hackers to attack & take over smartphones. Using this, the cybercriminals spy on the victim and monitor every action done by the victim.

MOBILE SERVICE CENTRES

A mobile repair shop may have a criminal who accesses private pictures or other data and uploads them on shady sites to make them viral. He may also use them for blackmail.

JUICE JACKING

Juice Jacking is one of the cyber-attacks in which cybercriminals create fake charging ports which are capable of copying data to/from smartphones. Charging ports at public places are prime areas for juice jacking.

Wi-Fi HACKING

Weak passwords to home Wi-Fi networks may enable a hacker to log into your network through the Wi-Fi connection in the vicinity. It will lead to internet time theft and breach of privacy

PHISHING SCAM

Hackers create fake websites which are clones of e-commerce/banking websites. It is used to steal usernames, passwords and money from the victims.

CUSTOMER CARE FRAUDS

Cybercriminals create fake websites for customer care and service centres and get listed in Google search results. This way, misleading results, fake helpline numbers etc. can be displayed, making the user believe them and fall prey to this scam.

GENERAL GUIDELINES FOR INTERNET USERS

Device Security (Computer/Mobile Phone)

Keep mobile phone operating system and other applications up-to-date.

Enable auto lock feature.

Take regular backup of important data.

Use encryption to secure data in your device.

Install antivirus application for mobile phone and computer.

Bluetooth device should be kept undiscoverable and should be turned off when not in use.

Avoid using 3rd party applications installation.

Do not jail break / root your phone.

Never follow links from unsolicited email or text messages.

Never access/transmit sensitive information when connected to the Internet at public at public places like shopping malls, cafes, etc.

Don't use same password for every-thing.

Cover webcams when not in use. .

Use anti-theft applications to protect from theft.

Browsing Internet

Always update the browser

Disable auto save password option.

Use strong passwords and change it once in a month.

Always logout after accessing your account.

Do not directly open the links from mails. .

Use ad blocker to restrict unneces-sary advertisements

Don't access any personal accounts or data while using free wi-fi

Check the last login details e-mail while accessing account.

Before opening e-mail attachments scan it through an updated anti-virus.

Be cautious about Tiny URLS in e-mail contents:

Use private browsing while using public computer

Do not download files from torrent sites

GUIDELINES ON SECURING SOCIAL MEDIA, AND OTHER APPLICATIONS

When setting up your phone you will need to activate a Google account on the handset. You can use your own **PARENTAL CONTROL USING GOOGLE PLAY STORE** Google account or create/use the account of your child. You will be enabling a PIN on the handset that can be used to set parental controls.

- Launch the Google "Play Store" application on your handset.
- Tap the menu button.
- From the pop-out menu scroll down and tap "Settings".
- In the "Settings" section scroll down and tap on "Parental controls".
- Enable parental controls by tapping on the radio button.
- You will be now prompted to create a PIN.
- You can now set restrictions for "Apps & games", "Films", "TV", "Magazines" and "Music" all of which are accessed via the Play Store.
- Now we will enable your handset to require the Google account password when making purchases. Return to the "Settings" menu within the "Play Store" app Scroll down and select "Require authentication for purchases".
- On the "Require authentication" pop-up you can select to require your Google account password for all purchases, open a 30-minute window where all purchases are allowed after putting in your password, or disable authentication entirely.
- Finally, we will now block the device from being able to install applications from services other than the "Play Store" where we have placed the restrictions. From your device's "home Screen" swipe down from the top of the screen and then select the settings icon.

Parental Control Apps available from Android

You can use the Family Link App to create a Google Account for your child. You can also use Family Link to add supervision to your child's existing Google Account.

Key features:

- Set screen time limit
- Allow or block apps
- Find your child's location

How to set up Family Link on a smartphone

- Start by downloading the Family Link app onto your device (Android or iPhone).
- If your child already has an account, Family Link will walk you through linking your and your child's account. As part of that process, your child may also need to down load the Family Link Child/Teen app on their phone to complete the process of linking the accounts.
- If your child does not already have a Google account (or Gmail), you can also create a Google Account for your child so that you can use Family Link. You can create a new Google account here. You can also use Family Link to create a Google Account for any child under 13.

- Once complete, children can sign in to their device with the new account. Once the accounts are linked, use Family Link to set digital ground rules for your family.

Set Screen Time Limit

- With a parent's device
- Open the Family Link app.
- Select your child.
- On the "Daily limit" card, tap Set up or Edit limits and follow the on-screen instructions.

Allow or Block Apps

The app will be blocked or unblocked in about 5 minutes, or once the device is connected to the internet. If your child is using the app at the time you block it, they'll get a one-minute warning to finish up before the app is blocked. The app is blocked on all of your child's Android devices.

- Open the Family Link app.
- Select your child.
- On the "Apps installed" card, tap More.
- Select the name of the app you want to allow or block.
- Turn Allow app on or off.

Find your child's location

If you're a parent, you can find your child's Android device location in the Family Link app.

- Open the Family Link app.
- Select your child.
- On the "Location" card, tap Set up.
- Turn on the settings required to find your child's location.
- Tap Turn on. It might take up to 30 minutes to find your child's device location.

How to prevent your child from changing their App Permissions

- Open the Family Link app.
- Select your child.
- Find the Device card.
- Tap View settings.
- Tap App permissions.
- Tap permission.
- Select only parents or your child and parents.

How to see your child's App Activity

You can see how much time your child spent using apps on their Android devices. Time is tracked when the app is open and shown on the screen, but not when the app is working in the background.

- Open the Family Link app.
- Select your child.
- Find the App Activity card.
- Tap Set up.
- After you turn on App Activity, you'll see your child's app activity in a few hours.

How to set Bedtime on your child's phone

- Open the Family Link app.
- Select your child.
- Find the Bedtime card.
- Tap Edit schedule.
- Follow the instructions on the screen to set bedtime.

How to Lock or Unlock your child's device

- Open the Family Link app.
- Select your child.
- On the card for one of your child's Android devices, tap Lock now or Unlock.

Application Safety

Safeguarding WhatsApp by 2 Factor Authentication

WhatsApp two-step verification is the most recommended feature which adds more security to your account. Once you enable the two-step verification, any attempt to verify your phone number on WhatsApp must be accompanied by the six-digit PIN that you created using this feature.

- Open WhatsApp Settings.
- Tap Account > Two-step verification > Enable.
- Enter a six-digit PIN of your choice and confirm it.
- Provide an email address you can access or tap Skip if you don't want to add an email address. We recommend adding an email address as this allows you to reset two-step verification, and helps safeguard your account.
- Tap Next.
- Confirm the email address and tap Save or Done.

How to prevent someone from adding you into groups without your permission

Go to WhatsApp Settings:
Android: Tap More options > Settings > Account > Privacy > Groups.
iPhone: Tap Settings > Account > Privacy > Groups.

Select one of the following options:

Everyone: Everyone, including people outside of your phone's address book contacts, can add you to groups without your approval.

My Contacts: Only contacts in your phone's address book can add you to groups without your approval. If a group admin who's not in your phone's address book tries to add you to a group, they'll get a pop-up that says they can't add you and will be prompted to tap Invite to Group or press Continue, followed by the send button, to send a private group invite through an individual chat. You'll have three days to accept the invite before it expires.

My Contacts Except...: Only contacts in your phone's address book, except those you exclude, can add you to groups without your approval. After selecting My Contacts Except… you can search for or select contacts to exclude. If a group admin you exclude tries to add you to a group, they'll get a pop-up that says they can't add you and will be prompted to tap Invite to Group followed by the send button to send a private group invite through an individual chat. You'll have three days to accept the invite before it expires.

If prompted, tap DONE or press OK.

Safeguarding Instagram

When your account is:

Public: your profile and publications are visible to everyone both outside and inside Instagram, even if the person who accesses them does not have an account on the said platform.

Private: Only followers you have approved can see the content you share, including your videos or photos on tag or location pages and your followers and followed account lists.

Note: If you are under the age of 16 when you sign up for Instagram, you have the option to choose between private and public accounts, but this is private by default.

Make your account private.

Instagram application for Android and iPhone:

- Tap or your profile photo at the bottom right to go to your profile.
- Tap at the top right, then Settings.
- Tap Privacy.
- Tap next to Private account to make it private.

Block or unblock someone from their profile.

- Tap their username in the news or stories post, or tap and search for their username to go to their profile.
- Tap ••• (iPhone or computer) or (Android) in the upper right.
- To block the account and any new accounts it can create, tap Block at the bottom to confirm the action.
- If you'd rather block only that account, tap next to Block [username). Tap Block again to confirm the action.

Two-factor authentication in Instagram

- Two-factor authentication is a security feature that helps protect your Instagram account and your password. If you set up two-factor authentication, you'll receive a notification or be asked to enter a special login code when someone tries logging into your account from a device we don't recognize.

To turn on two-factor authentication from the Instagram app:

- Tap on your profile picture in the bottom right to go to your profile.
- Tap in the top right, then tap Settings.
- Tap Security, then tap Two-Factor Authentication.

Safeguarding Facebook

Verify every Facebook contact.

- Make sure that the person you're talking to is the person you think they are. Try to verify their identity.

Protect your banking and financial information.

- Never disclose anything about your bank accounts, credit cards, debit cards, or other financial information on Facebook.

Keep your password secure.

- Taking a little extra care over your password can be a vital element in your Facebook security.
- Create a strong password that will be difficult for others to guess.
- Ideally, your password should use a mixture of letters, numbers and symbols.
- Remember to change your password frequently.
- Don't use the same password for Facebook and other websites. If the security of your password is compromised on one site, it may then be used to access your Facebook account.

Log out of Facebook when you use a computer you share with other people.

Enable Two Factor Authentication.

- Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you'll be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device we don't recognize. To turn on or manage two-factor authentication:
- Go to your Security and Login Settings.
- Scroll down to Use two-factor authentication and click Edit.
- Choose the security method you want to add and follow the on-screen instruc tions.
- When you set up two-factor authentication on Facebook, you'll be asked to choose one of three security methods:
  - Tapping your security key on a compatible device.
  - Login codes from a third-party authentication app.
  - Text message (SMS) codes from your mobile phone.

Control who can see what's posted on your timeline.

- Facebook has an option that allows you to select exactly who can see your posts. This is available via the Privacy Check-up and Privacy Shortcut sections, but for the purpose of this post, we'll stick with the regular privacy settings options.
- To limit who can see what you post in the future, start by clicking on the arrow in the top right corner of the toolbar and select Settings & Privacy > Settings > Privacy.
- Under Your Activity, the first option is who can see your future posts? Click on Edit next to this.

Now select from:

Public (this means everyone)

Friends

Friends except…

(all of your friends except for any you purposefully omit)

Specific friends

(only those people you choose from your existing list of friends)

Only me

Pick whichever option works for you. Public should probably be avoided and Only me seems a bit pointless, and then that setting will apply for all your future posts.

- Check where you're logged in.

  Have you accidentally left yourself logged into your Facebook account on a device that can be accessed by your family, lost a device, or sold one without logging out of Facebook?

  If so, you'll want to review which devices are logged in and do something about it!

- On the Security and Login page, look for the Where You're Logged In section, which may already be displaying one or two devices. Click on See More to see a full list of devices that are logged in.
- You won't be able to log out of the session you are currently using but you can do so for one or more other devices.
- You can either select Log out Of All Sessions or you can click the column of three dots next to a specific entry to log out of a particular session.
- If you see any devices you don't recognize here, you can notify Facebook that the device in question is not yours and you will be walked through steps to secure your account.

Best practices for Secure Online Classes in Google Meet

While in the meeting, you can invite others to join. For meetings organized through personal Google accounts, only the meeting organizer can admit participants.

- Reporting a Member - during a meeting
- Join a Meet video call.
- Click More.
- Click Report a problem.
- Describe the issue or share your ideas.
- Select Include screenshot to help identify the issue.
- Click Send.

- Reporting a Member - after meeting
- In a web browser, enter https://meet.google.com/.
- Click Feedback.
- Describe the issue or share your ideas.
- Select Include screenshot to help identify the issue.
- Click Send.

Best practices for Secure Online Classes in Zoom

Send Out Meeting Invites.

- One good practice to implement is to send attendees meeting invites. You can do this through Microsoft Outlook and also Gmail.

Enable the Waiting Room Feature.

- By turning on the Waiting Room feature, you'll be able to control who enters your meeting.

- Here's how to enable the Waiting Room feature:
- Go to "Account Management" > "Account Settings"
- Under "Security" if the Waiting Room feature is disabled, you toggle it on.
- If you want to make this required for everyone on the Zoom account, click the lock to make it mandatory.

Require a Passcode.

A good way to prevent unwelcome guests from joining your Zoom meeting is to require participants to enter a passcode before logging into the meeting

- Here's how to require a passcode:
- Go to "Account Management" > "Account Settings"
- Under "Security" you can toggle on the passcode feature if it's not already Enabled.
- You can also lock this feature so that passcode will be required for all of your account users whenever they set up a meeting or webinar.

Once everyone's there, Lock the Meeting.

Before you start the meeting, check to see if everyone's there, and lock the meet ing to prevent anyone else from joining in. This is another helpful way to prevent "Zoom Bombing" so there will be no surprise guests.

- Here's how to lock your Zoom meeting:
- Look down the bottom of the Zoom meeting window and click "Participants".
- From here, you'll see a button that says "Lock Meeting" that you can select.

Place All Participants on Mute.

- To prevent any disturbances during a team training, meeting, or class, you can place all participants on mute as soon as they join. This will help to minimize distractions.

Here's how to mute all Zoom participants:

- Look at the bottom of your meeting screen.
- Click on the "Participants" button.
- Click "Mute All".
- If you want participants to be able to unmute themselves during the meeting,
- you can select the option "Allow participants to unmute themselves".

Turn off Annotations.

If you want to prohibit students from writing or drawing on Zoom's whiteboard or employees from adding notes to a slideshow, you can do this by turning off annotations. This will prevent unwanted activity during your meeting that could be distracting or a disruption.

Here's how to turn off annotations in Zoom:

- Go to "Account Management" > "Account Settings".
- Click on the tab that says "Meeting".
- Look under "Meeting (Basic)" to see if Annotations are currently enabled. If so, you can toggle this feature off.
- If you want only the person sharing their screen to add annotations, you can select the corresponding box for this feature. This can be helpful if you call on a student to show their work or an employee to brainstorm for the group.

Disable the Private Chat Feature.

- To help keep the meeting more focused, you can also disable the private chat feature. For employers, this helps to take away distractions from important conversations, and for teachers, this helps to keep students focused on class (and less on chatter).

Here's how to disable the private chat feature in Zoom:

- Under the Meeting Controls, click on "Chat".
- Once the chat window has opened, click "More" and select the appropriate option. If you don't want participants to chat with anyone, select "No one". If you want participants to chat only with the host, select "Host-only".

Manage Who Can Share Their Screen.

- Prevent unexpected distractions or screen sharing by managing who can share during a meeting, training session, lecture, or even social gathering. This way you can keep everyone focused and centred as well as prevent unwanted information shared with those in the meeting.

Here's how to manage who can share their screen in Zoom:

- In your host controls next to the "Share Screen" option, click on the arrow.
- Next, click "Advanced Sharing Options".
- Under the "Who can share?" option, select "Only Host".

Keep Zoom updated.

- Remember to keep the platform updated as you use it. This will help to ensure you have the latest version and are up to date with any security changes.

Best practices for Secure Online Classes in WebEx

Restrict access to the meeting.

- Lock the meeting once all attendees have joined the meeting. This practice prevents more attendees from joining. Hosts can lock or unlock the meeting at any time while the session is in progress.
- To lock a meeting that you're currently hosting, select Meeting > Lock Meeting.

Validate the identity of all users in a call.

- Accounting for every attendee by using a roll call is a secure practice. Ask users to turn on their video or state their names to confirm their identity.

Share application, not screen.

- Use Share > Application > instead of Share > My Screen to share specific applica tions and prevent accidental exposure of sensitive information on your screen.

Do not allow join before the host.

- Consider disabling the join before host options for your site. To do this, Sign in to WebEx Site Administration, and navigate to Configuration > Common Site Settings > Options > Security Options.
- To prevent attendees from joining before the host, uncheck the following boxes: Allow attendees or panellists to join before host (Meetings, Training and Events) The first attendee to join will be the presenter (Meetings)

Restrict unauthenticated users.

- Allow attendees who have signed in to enter an unlocked Personal Room, but require unauthenticated attendees to wait in the lobby of the unlocked Personal Room until the host manually admits them. To do this,
- Sign in to WebEx Site Administration, and navigate to Configuration > Common Site Settings > Options.
- In the Site Options section, scroll to Personal Room Security to view the following option:
- Signed-in attendees can enter an unlocked room, but unauthenticated attend ees must wait in the lobby until the host manually admits them.
  This is the minimum recommended level of security. It provides the host with a list of users who are unauthenticated and allows the host to allow individual users who are legitimate attendees while preventing those who aren't.

Securing Microsoft Teams Meetings

- Use proper security labels while creating a Team Meeting.
- Use the Lobby feature.
- Enable private channels within a team.
- Create Specific groups of participants instead of Open meetings.
- Control the Access Levels.
- Regularly monitor user activity.
- Choose the right options before starting a meeting.
- Securing Files in Microsoft Team.

GUIDELINES FOR PSYCHOLOGICAL HANDLING OF CHILDREN INVOLVED/VICTIMISED IN CYBER CRIMES

WHY AND HOW TO HELP PSYCHOLOGICALLY?

Any adolescent cyber-crime victims are prone to suffer fear and pressure due to the anonymity of the victimizers and their intentions. There will be a constant worry about the after-effects, feeling worthless, difficulty in trusting anyone immediately and reduced attention. While a victim is under pressure, s/he is more likely to exhibit violent behaviour or a withdrawn behaviour like feelings of frustration, hurt, sadness and grief, feelings of being bullied, humiliated, excluded and insecure; angry, disgusted or disappointed and even suicidal ideations. So,

- Be calm and be with the adolescent.
- Be empathetic towards the victim and family.
- Give emotional support - do not blame the victim.
- Do not be angry or panicked, but act immediately.
- Accept the fact that worrying is normal and help the victim to rebuild trust.

Adolescent victims or addicts who are repeatedly exposed to unhealthy cyber-space may lessen their assertiveness skills and decision-making skills. They would often feel lonely and worthless. So, this explains why s/he would not inform anyone about their

experience and try to resolve the issues by themselves and end up in more trouble. Considering parental reputation and devaluing others' dignity can prevent from taking action. The feeling of being attacked or anticipating a negative consequence of legal actions can be debilitating. The difficulty in trusting or facing anyone at this stage is commonly seen. So,

- Assure them that help is accessible.
- Give the adolescent a chance for honest open discussion "it happens; together we shall deal with it".
- Encourage to seek legal help.

Repeated exposure to obscene content during adolescence may develop recurrent obsessions, unusual sexual practices, distorted thought patterns, poor ability to tolerate stress, become vulnerable to abuse. Low mood, emotional issues and poor attention may lead to academic decline and troubles in relationships. Declined self-care, negative sense of self and anxiety can be seen in them. The child suffers from guilt, shame, feels mentally frustrated and upset. A high risk of depression, social withdrawal and suicidal ideas can be predicted. Children who are having internet addiction, use the virtual fantasy world to connect with real people through the internet, as a substitution for real-life human connection, which they are unable to achieve normally. The ongoing Covid 19 pandemic made adolescent students spend more time online maintaining connectivity as social interaction is limited. So,

- Encourage to seek help from a mental health professional.
- Skills associated with coping with stress and emotions can be taught with the help of a mental health professional.

Adolescence is a vulnerable period for the development of problem behaviours, including substance use initiation and delinquency. Ignorance of the negative consequences of his actions, impulsivity and risk-taking behaviour can be the predictive factors of his dissocial behaviour. Children at this stage tend to take care of their personal interests and ignore others' interests. In the cyber world, a lot of misbehaviours and illegal activities are being conducted because the actors think that their identity is securely hidden and may not be easily caught by the authority. Adolescence is a vulnerable period for impulsivity, risk-taking behaviours and disregarding consequences. Cyber pornography affects personality, family relationships, etc., and it can also cause negative social issues, such as adolescent crime, sexual behaviour, and child abuse and can engage in many sex-related online activities (e.g., Internet sex, Internet sexual harassment, etc. These children also need help, so,

- In case if the adolescent is the offender and does not have any remorse or concerns regarding the event, behavioural management needs to be carried out, with the help of mental health professional.
- Ensure expert support as long as needed.

It is found that adolescents with internet addiction often feel lonely and worthless. Engaging in crimes can be self-rewarding for the adolescent. They would commit crimes intentionally so long as they are not being caught. During the pandemic, education and related activities changed to an online platform which might have contributed to a situation where adolescents are not able to open up to people about negative experiences. So, this explains why he did not inform anyone and tried to resolve the issues by himself, failed and was victimised. The reduction of time spent together with available

people at home might have increased the time spent online to have real-life human connections, which they are unable to achieve normally. Adolescence is a period when they want to be heard the most, utmost creative phase and the period where they are moulded as a person.

- Convince the victim the need to inform parents and teachers whenever they feel uncomfortable online.
- After the acute crisis, convince the victim about the safe use of technology and assertiveness skills.
- Give support and educate the family about the safe use of the internet.
- Encourage the victim to help trace the offender, if any, and do damage control.
- Help him cope with interpersonal situations.
- Help him identify his emotions.
- Help the child to feel valued in a social group.
- Educate the parents to communicate with their children compassionately.

BEING SAFE ONLINE - GUIDELINES FOR PARENTS AND CHILDREN

Children's rights are human rights, to protect the child as a human being. All over the world, various laws and regulations have been passed for the safety of children. The United Nations Convention on the Rights of the Child (UNCRC) is an internationally binding human rights agreement. The convention has 54 articles, 42 of which set out the rights of children and young people. UNICEF is a strong advocate of child rights and works in numerous countries across the world. In India, the Indian constitution of 1950 asserts that everyone has the right to life, liberty and the security of persons and that no person shall be deprived of his life or personal liberty. The National Commission for Protection of Child Rights is an Indian statutory body established by an Act of Parliament, the Commission for Protection of Child Rights Act, 2005.

The **National Cyber Security Policy**, 2013 addresses the prevention, investigation and prosecution of cybercrimes, including those against children and strengthening law enforcement agencies to investigate cybercrimes.

Despite the numerous international human rights treaties and domestic laws which protect child rights, we are struggling to create the right atmosphere and environment for children. The year 2020 showed us a different life where many people lost their lives and the struggle for breathing oxygen was most felt. We faced lockdowns all over the world and this brought us to stay indoors within the four walls of our homes. Though the middle-aged and elderly were affected, the most affected were the children and youth who were cut off from their active, social and friendly atmosphere to being solitary and meeting their classmates online. The internet which was otherwise mostly used by office goers and senior students is now accessible to children of all ages. Parents have been forced to shell out money and buy gadgets for their children to ensure they have the right learning tool. The internet provides an open world of information and technology to anyone accessing it, however, the security of a person is also compromised. People of all ages are prone to online abuse but children are soft targets for predators who have the benefit of anonymity.

The crimes against children vary from cyberbullying, sexting, honey trapping which may also end up succumbing to the demands of the predator fearing ostracization from society. Direct crimes on a child may be shared by the child to their friends or family but online crimes have no face and the child fears no one would trust them. Many times the children themselves fall into the traps.

One needs to understand when there is an opportunity, responsibility comes along with it. It's not only the responsibility of the child but also of the parents, the authorities and the society as a whole. The child needs to understand their responsibilities of using the phone and the parents should guide them and assure them that they are there for them. The right action needs to be taken if something negative happens. Children need to be aware of the internet and how it functions - any data, photo, contact put online is accessible to people from across the globe. While using social websites - ensure not to befriend anyone unknown to them, avoid sending personal details, address, school name and photos especially nude ones. In case the child gets involved with someone and feels uncomfortable, they should immediately speak to someone they are comfortable with at home or school. One should understand that predators find the weaknesses of a person and often look for people who have a void in their lives and are emotionally vulnerable.

> In 2020, a study by the Internet Watch Foundation confirmed 1.5 lakh web pages as having child sexual abuse material. There was a 77% rise in the proportion of websites with child sexual abuse imagery.

The parents need to ensure that they are aware of the activities of the child especially the websites, emails or messages on their child's phone. They need to observe the behaviour of the child as those facing trauma exhibit self-destruction, privacy and are withdrawn. If something seems out of place, the parent should take the child in confidence and support them and help prevent unfortunate situations. Parents should first block the predator's contact on the child's phone and contact the police. Counselling sessions should also be organised for the child to avoid self-harm by the child.

The following pages showcase the legal aspect of support when a child and family are faced with abuse. The details of the Kerala Police Act 2011, the Juvenile Justice Act and similar acts which are for the protection of children and the young are mentioned below:

LAWS THAT ARE APPLICABLE IN CYBERCRIMES IN A NUTSHELL

The POCSO Act			
Section of Law	**Offence mentioned in the section**	**Penal Sections**	**Commonly reported offences under this section**
Section 11	Sexual harassment	Section 12	Cyber Bullying, Cyber Stalking
Section 13	Use of child for pornographic purposes.	Section 14	Sexting, Cyber Grooming, Child Pornography
Section 15	Storage or possession of pornographic material involving a child.	Section 15(1), 15(2), 15(3)	Sexting, Child Pornography
Section 22	Punishment for false complaints or false information.	Section 22, 22(2), 22(3)	
Section 23	Procedure for media	Section 23(4)	

The Information Technology Act			
Section 43	Penalty and compensation for damage to the computer, computer system, etc.	Section 43 & 66	
Section 66	Computer-related offences.	Section 66	Sextortion
Sec 66B	Punishment for dishonestly receiving stolen computer resources or communication devices.	Sec 66B	Theft
Sec 66C	Punishment for identity theft.	Sec 66C	Hacking
Sec 66D	Punishment for cheating by personation by using computer resource.	Sec 66D	Impersonation
Sec 66E	Punishment for violation of privacy.	Sec 66E	Sexting, Sextortion, Honey Trap
Sec 66F	Punishment for cyber terrorism.	Sec 66F	Radicalization
Sec 67	Punishment for publishing or transmitting obscene material in electronic form.	Sec 67	Cyber Stalking, Sexting, Sextortion, Picture Morphing
Sec 67A	Punishment for publishing or transmitting of material containing sexually explicit acts, etc., in electronic form.	Sec 67A	Cyber Stalking, Sexting
Sec 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit acts, etc., in electronic form.	Sec 67B	Sexting, Cyber Grooming, Child Pornography
Sec 72	Penalty for Breach of confidentiality and privacy.	Sec 72	Cyber Stalking, Sextortion
The Indian Penal Code (IPC)			
Sec 107	Abetment of a thing.	Sec 109	
Sec 124A	Sedition		
Sec 153A	Promoting enmity between different groups on the ground of religion,	Sec 153A(1), 153A(2)	
	race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.		
Sec 153B	Imputations, assertions prejudicial to national integration.	Sec 153B(1), 153B(2)	
Sec 204	Destruction of a document to prevent its production as evidence.	Sec 204	
Sec 292	Sale, etc., of obscene books, etc.	Sec 292(2)	Sextortion, Picture Morphing
Sec 293	Sale, etc., of obscene objects to a young person	Sec 293	
Sec 305	Abetment of suicide of child or insane person.	Sec 305	
Sec 354	Assault or criminal force to woman with intent to outrage her modesty.	Sec 354	
Sec 354A	Sexual harassment and punishment for sexual harassment.	Sec 354A(1)(i), (ii), (iii) & (iv), Sec 354A(3)	Cyber Bullying, Cyber Stalking, Sextortion
Sec 354B	Assault or use of criminal force to woman with intent to disrobe.		Cyber Stalking, Sextortion

Sec 354C	Voyeurism		Cyber Stalking, Sextortion
Sec 354D	Stalking		Cyber Bullying, Cyber Stalking, Sextortion
Sec 361	Kidnapping from lawful guardianship.	Sec 363	Taking a child from the custody of a parent
Sec 363A	Kidnapping or maiming a minor for purposes of begging.	Sec 363A(1), 363A(2)	
Sec 366	Kidnapping, abducting or inducing a woman to compel her marriage, etc.		
Sec 366A	Procuration of a minor girl.		
Sec 369	Kidnapping or abducting a child under ten years with the intent to steal from its person.		
Sec 370	Trafficking of person.	Sec 370(2), 370(3), 370(4), 370(5), 370(6), 370(7)	Cyber Grooming
Sec 370A	The exploitation of a trafficked person.	Sec 370A(1), 370A(2)	
Sec 372	Selling minors for purposes of prostitution, etc.		
Sec 373	Buying minors for purposes of prostitution, etc.		
Sec 383	Extortion	Sec 384	Honey Trap
Sec 415	Cheating	Sec 417	
Sec 419	Punishment for cheating by personation.		
Sec 420	Cheating and dishonestly inducing delivery of property.		Honey Trap
Sec 463	Forgery	Sec 465	
Sec 468	Forgery for purpose of cheating.	Sec 468	
Sec 469	Forgery for purpose of harming reputation.		
Sec 470	Forged document	Sec 471	
Sec 499	Defamation	Sec 500	Cyber Bullying, Cyber Stalking, Trolling, Sextortion, Picture Morphing
Sec 503	Criminal intimidation	Sec 506	Cyber Bullying, Cyber Stalking, Sextortion, Honey Trap
Sec 509	Word, gesture or act intended to insult the modesty of a woman.	Sec 509	Cyber Bullying, Cyber Stalking, Sextortion, Picture Morphing
The Kerala Police Act, 2011			
Section 119(b)	Punishment for atrocities against women.	Section 119(b)	Cyber Stalking, Cyber Pornography
Section 120(o)	Penalty for causing nuisance and violation of public order.		Cyber Bullying
The Juvenile Justice Act, 2015			
Section 74	Prohibition on disclosure of the identity of children.	Section 74	
Section 75	Punishment for cruelty to a child.	Section 75	
Section 76(1) & (2)	Employment of child for begging.	Section 76(1) & (2)	

Section 77	Penalty for giving intoxicating liquor or narcotic drug or psychotropic substance to a child.	Section 77	
Section 78	Using a child for vending, peddling, carrying, supplying or smuggling any intoxicating liquor, narcotic drug or psychotropic substance.	Section 78	
Section 79	The exploitation of a child employee.	Section 79	
Section 80	Punitive measures for adoption without following prescribed procedures.	Section 80	
Section 81	Sale and procurement of children for any purpose.	Section 81	
Section 83(1)	Use of children by militant groups or other adults.	Section 83(1)	
Section 83(2)	Use of children by militant groups or other adults	Section 83(2)	
Section 84	Kidnapping and abduction of a child.	Section 84	
Section 85	Offences committed on disabled children.	Section 85	
Section 87	Abetment.	Section 87	
The Immoral Traffic (Prevention) Act, 1956			
Section 5	Procuring, including or taking a person for the sake of prostitution.	Section 5	
Section 8	Seducing or soliciting for the purpose of prostitution.	Section 8	
The Child and Adolescent (Prohibition And Regulation) Act, 1986			
Section 14	Penalties	Section 14(1), 14(1)A, 14(1)B, 14(2), 14(2)A, 14(3)	
Indecent Representation of Women (Prohibition) Act, 1986			
Section 3	Prohibition of advertisements containing indecent representation of Women	Section 3	Sextortion, Picture Morphing
Section 4	Prohibition of publication or sending by post of books, pamphlets, etc; containing indecent representation of women.	Section 4	Sextortion, Picture Morphing
Section 6	Penalty	Section 6	Sextortion, Picture Morphing
The Copyright Act, 1957			
Section 63	The offence of infringement of copyright or other rights conferred by this Act.	Section 63	
Section 63A	Enhanced penalty on second and subsequent convictions.	Section 63A	
Section 63B	Knowing the use of infringing copies of a computer programme to be an offence.	Section 63B	
Section 66	Disposal of infringing copies or plates for purpose of making infringing copies.	Section 66	
Section 68	Penalty for making false statements for the purpose of deceiving or influencing any authority or officer.	Section 68	

The Young Persons (Harmful Publications) Act, 1956			
Section 3	Penalty for sale, etc., of harmful publications.	Section 3	
The Scheduled Castes and The Scheduled Tribes (Prevention of Atrocities) Act, 1989			
Section 3	Punishments for offences of atrocities.	Section 3	

The Cinematograph Act, 1952

Offence mentioned in the section	Penal Sections	Commonly reported Offences under this section
Penalties for contravention of this part.	Section 7	Cyber Piracy

The Code of Criminal Procedure, 1973

Section of law	Victim Compensation Scheme
Section 357A	

CONTACT DETAILS OF HELPLINE NUMBERS FOR CHILDREN

Sl. No.	Helpline	Phone Number/Web Address	Nature of complaint that can be made
1.	Aarambh India Hotline	+918104461284 www.aarambhindia.org info@aarambhindia.org	Complaints on online child sexual abuse
2.	Bachpan Bachao Andolan	1800 102 7222	Toll-free – reporting violence against children
3.	Bhumika	1800 425 2908	Complaints regarding women protection
4.	Child Welfare Committee	Mentioned district wise contact details in the below table	To ensure care, protection, treatment, development, and rehabilitation of children in need of care & protection
5.	Childline	1098	24-hour, free, emergency phone service for children in distress
6.	Chiri Helpdesk	9497900200	Complaints regarding help and assistance for children
7.	Crime Stopper	1090	To seek help from Police to prevent any crime without disclosing the identity of the complainant
8.	DCPU (District Child Protection Unit)	Please see the district wise contact details mentioned below	Protection of rights and interests of children
9.	DISHA (Toll-free Tele-health Helpline)	1056 Toll-free: 1800 425 11222	State Health helpline
10.	DLSA (District Legal Service Authority)	Mentioned district wise in the table below	Free legal aid for children, women, and other weaker sections of society
11.	Doctors desk of Nanma	8943270000, 8943160000	Mission Better Tomorrow - Nanma Doctors desk for citizens in quarantine from 9 AM to 6 PM
12.	ICDS (Integrated Child Development Services)	Contact Anganwadi concerned	For ensuring Healthcare, education, immunization of children of the age group of 0-6 years

13.	ICPS (Integrated Child Protection Scheme)	0471-2342235	ICPS, Poojappura, Thiruvananthapuram
14.	Juvenile Justice Board	Contact district unit concerned	To ensure the protection of the rights of children
15.	Kerala State - cyber nodal	9497976005, 0484 2630238 https://cyberdome.kerala.gov.in/reportus.html	Nodal cyber Cell Cyberdome/ cell Aluva, Ernakulum
16.	Kerala State Commission For Protection of Child Rights	childrights.cpcr@kerala.gov.in Phone: 0471 232 6603 http://www.kescpcr.kerala.gov.in/	Inquire into complaints of violations of child rights
17.	KIRAN Helpline	18005990019	National level mental health support) central government
18.	KLSA (Kerala Legal Service Authority)	0484-239-6717	Free legal aid for children, women, and other weaker sections of society
20.	National Cybercrime reporting cell/portal	www.cybercrime.gov.in	Complaints about cybercrimes only with special focus on cybercrimes against women and children
21.	NCPCR - National Commission for the Protection of Child Rights (NCPCR)	A PANIC Button- POCSO E-Box - http://www.ncpcr.gov, http://www.ncpcr.gov.in	Child sexual abuse complaint Address- 5th Floor, Chandralok Building, 36, Janpath, New Delhi 110001
22.	Nirbhaya	0471-3243000, 3244000	Protection of rights and interests of women & children
23.	NTCP (National Tobacco Control Programme)	In District hospitals	De-addiction service
24.	ORC (Our Responsibility to Children)	0471 234 2235	Complaints regarding the protection of children
25.	Police	112	In the event of facing any distress situation
26.	Police	0471-324 3000/4000/5000	Police Helpline (central)
27.	Police	122	Medicine delivery for citizens (by highway Police)
28.	Sakhi: one-stop centre for all assistance to women	Mentioned district wise in the table below	Protection of women's rights, counselling and free legal aid
29.	State Women and Child Department	directorate.wcd@kerala.gov.in , 0471-2346534, 2346508	The state government machinery that focuses on the welfare of women and children
30.	Thanal- Kerala State Council for Child Welfare	1517	Rescue and rehabilitation of children in distress
31.	Vimukthi (Kerala Excise Department)	Mentioned district wise in the table below	De-addiction service

DISTRICT WISE CONTACT DETAILS OF OFFICES IN SUPPORT FOR CHILDREN

Sl. No.	District	District Child Protection Unit	Child Welfare Committee	District Legal Services Authority	Child Line Collab Partners
1	Trivandrum	0471- 2345121	7907669163	0471- 2579057	0471-2339159/60, 9489302455
2	Kollam	0474- 2791597	9387313050	0474- 2791399	0474 2760327, 9747808107
3	Pathanamthitta	0468- 2319998	9447563609	0468- 2220141	0468 2224375, 2224385, 9447020936
4	Alappuzha	0477- 2241644	9446573248	0477- 2262495	9895729311, 8113801098
5	Kottayam	0481- 2580548	9447348293	0481- 2302422	9544389433 /9446563000
6	Idukki	0486- 2200108	9447092950	0486- 2255383	9961062241
7	Ernakulam	0484- 2426892	9846204429	0484- 2344223	0484 2204718, 2205198, 9847331098
8	Thrissur	0487-2364445	9495926137	0487- 2363770	808942128
9	Malappuram	0483- 2978888	9447227340	0483- 2762220	04832730739,9995118 595
10	Palakkad	0491- 2505791	9446531809	0491- 2505665	8281297229
11	Kozhikode	0495- 2378920	8593986239, 9747532959	0495- 2366044	0495 2725899, 9447090077
12	Wayanad	0495- 2378920	9847848567	0493- 6207800	9562911098
13	Kannur	0490- 2326199	9446680362	0490- 2326766	0497-2708474, 2706474, 9895515250
14	Kasargod	0499- 4256990	9495653810	0499- 256189, 0499- 4255189	9495596433

DISTRICT LEVEL - CHILD PROTECTION AGENCIES

Sl. No.	District	District Child Protection Unit	Child Welfare Committee	District Legal Services Authority	Childline Collab Partners
1	Trivandrum	0471- 2345121	7907669163	04712579057	0471-2339159/60, 9489302455
2	Kollam	0474-2791597	9387313050	04742791399	0474 2760327, 9747808107
3	Pathanamthitta	0468- 2319998	9447563609	04682220141	0468 2224375, 2224385, 9447020936
4	Alappuzha	0477-2241644	9446573248	04772262495	9895729311, 8113801098
5	Kottayam	0481-2580548	9447348293	04812302422	9544389433 /9446563000
6	Idukki	0486-2200108	9447092950	04862255383	9961062241
7	Ernakulam	0484-2426892	9846204429	04842344223	0484 2204718, 2205198, 9847331098
8	Thrissur	0487-2364445	9495926137	04872363770	808942128
9	Malappuram	0483-2978888	9447227340	04832762220	04832730739, 9995118595
10	Palakkad	0491-2505791	9446531809	04912505665	8281297229
11	Kozhikode	0495- 2378920	8593986239, 9747532959	04952366044	0495 2725899, 9447090077
12	Wayanad	0495-2378920	9847848567	04936207800	9562911098
13	Kannur	0490-2326199	9446680362	04902326766	0497-2708474, 2706474, 9895515250
14	Kasargod	0499-4256990	9495653810	04994256189, 04994255189	9495596433

Sl. No.	District	One-Stop Centre - (OSCs) are intended to support women affected by violence, in private and public spaces, within the family, community	Kudumbasree (Snehitha Gender Help desk) - Snehitha provides immediate help, shelter, counselling and legal assistance to the victim of	District Mental Health- 9 am to 4 pm -Psychosocial support helpline in Kerala	Mental health Support District Helpline (Social Justice department / DCPU) Child	CHILDLINE -1098 Kerala Partner NGO for Emergency rescue and relief (N-Nodal, C-collab, S-Support organisation)
1	Trivandrum	0471-2741699	04712430661	9846854844	DPMSU-0471 277900, 9188610100, 1077 (toll free), 9846854844	N -Loyola Extension Services, 0471-2595097, C-Don Bosco Nivas C-9895743287 Trivandrum Social Service Society (TSSS) 0471-2727123,
2	Kollam	04742957827, 6282930869	04742799661	0474 2740166, 8281086130	DPMSU & Home Care-0475 2964009, 7592006857	C-Quilon Don Bosco Centre: 0474 2760327, 9747808107
3	Pathanamthitta	9495161699	04734250244	8281113911	0468 2228220, 2322515, 8281574208, 944798316	C-C- BODHANA, S-Punalur Social ServicSociety, CHILDLINE Ph: 0468 2224375, 2224385 Mob: 9447020936
4	Alappuzha	9495326115	04772230912	0479 2344474	7593830443, 0477 2967544	C- Alleppey Diocese charitable and social welfare society, Ph: 9895729311, 8113801098
5	Kottayam	9400789701	04812538555	9539355724	9188610014, 9188610016, 0482 2304800, 0481 2583200, 0481 2566100, 0481 2566700, 0481 2561300	C- Vijayapuram social service society Mob-9544389433 /9446563000
6	Idukki	04862296069	04862236679	0486 2226929, 9496886418	0486 2226929, 8330057178	C- Vosard regional office 9961062241
7	Ernakulam	85477 10899	04842428745	0484 2351185 9846996516	0484 2368702, 2368702, 2368902	N: Rajagiri College of Social Sciences Ph: 0484-2532099 / 0484-2555564, Collab -Don Bosco Snehabha-van 0484-2231009
8	Thrissur	4802833676	04872382573	0487 23831553	8129701884	Nodal- Vimala College 0487-2330351,2332080

9	Malappuram	4933297400	04832770500	0491253323	7593843617, 7593843625	C- Sheshy Charitable Society, Phone: 04832730739 Mobile: 9995118595
10	Palakkad	8547202181	04912505111	7593843617, 7593843625	0491 2533323	N- Mercy College C- Samagra
11	Kozhikode	4952732253	04952371100	9495002270	7736050066, 9400866004, 9744109070, 8590919025	N- Farook College 0495-2440766, 9745836848, C- Association for the Welfare of the Handicapped 0495-2725777, Childline Kozhikode Ph:0495 2725899 Mob: 9447090077
12	Wayanad	04936-202120	04936202033	9400348670	9400348670	C/N - JVALA Kalpetta North, 04936203574 / 206036, Childline Wayanad, JVALA, Ph: 04936205264 / 206036 9562911098
13	Kannur	04902367450, 7306996066	04972721817	04972734343 9495142091	9495142091, 0497 2734343	N- Don Bosco College , C- Thalssery Social Service Society C- AWH
14	Kasargod	9400088573, 04994255266	04672201205	9072574748 9447447888	9946000493, 9946000293	N- Mar Thoma College of Special Education

CONTACT DETAILS

Sl. No	Districts	Vimukthi	ICDS	De-addiction	
				Phone No.	Nodal Officers (Excise Circle Inspector)
1.	Thiruvananthapuram	9447178053, 0471-2473149	0471-2341001	0471- 2222235	9400069409
2.	Kollam	9447178054, 0474-2767822	8281999018, 04742793069	0474-2512324	9400069441
3.	Pathanamthitta	9447178055, 0468- 2222873	8281999019, 04682221430	0473-5229589	9400069468
4.	Alappuzha	9447178056, 0477-2252049	8281999021, 04772251200	0479-2452267	9400069488
5.	Kottayam	9447178057, 0481-2562211	8281999022, 04812561677	0482-2215154	9400069511
6.	Idukki	9447178058, 04862-222493	0486-2221868, 8281999023	0486-2232474	9400069532
7.	Ernakulam	9447178059, 0484-2390657	0484-2423934	0485-2832360	9400069564
8.	Thrissur	9447178060, 0487-2361237	8281999025, 04872321689	0480-2701823	9400069589
9.	Palakkad	9447178061, 0491-2505897	8281999027, 04912505780	0492-4254392	9400069588
10.	Malappuram	9447178062, 0483-2734886	0483-2730084, 82819999026	0493-1220351	9400069646
11.	Kozhikode	9447178063, 0495-2372927	8281999294, 04952375760	0495-2365367	9400069675
12.	Wayanad	9447178064, 04936-248850	8281999029, 04936204833	0493-6206768	9400069663
13.	Kannur	9447178065, 04972- 706698	0497-2700707, 9400933394	0498-5205716	9400069695
14.	Kasaragod	9447178066, 04972-705470	04994 - 256660	0467-2282933	9400069723

Published by

CHILDREN AND POLICE
STATE RESOURCE CENTRE
A CaP for CARE & PROTECTION