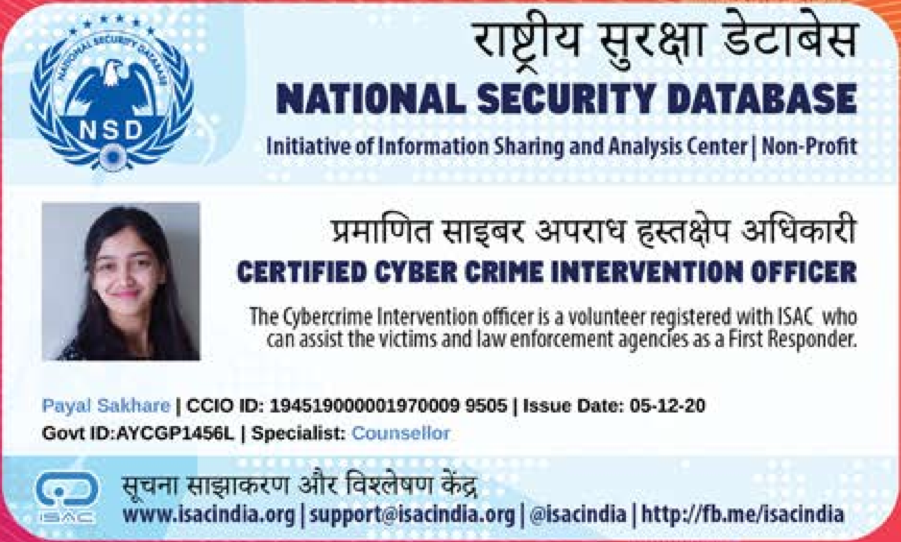
CERTIFIED CYBERCRIME INTERVENTION OFFICER



राष्ट्रीय सुरक्षा डेटाबेस

NATIONAL SECURITY DATABASE

Initiative of Information Sharing and Analysis Center | Non-Profit

प्रमाणित साइबर अपराध हस्तक्षेप अधिकारी

CERTIFIED CYBER CRIME INTERVENTION OFFICER

The Cybercrime Intervention officer is a volunteer registered with ISAC who can assist the victims and law enforcement agencies as a First Responder.

Payal Sakhare | CCIO ID: 194519000001970009 9505 | Issue Date: 05-12-20
Govt ID:AYCGP1456L | Specialist: Counsellor

सूचना साझाकरण और विश्लेषण केंद्र
www.isacindia.org | support@isacindia.org | @isacindia | http://fb.me/isacindia

Detect early signs of problems in children and teeenagers affected by their online activties. Learn about cybercrimes and cyber laws to protect your loved ones and act as a first responder.

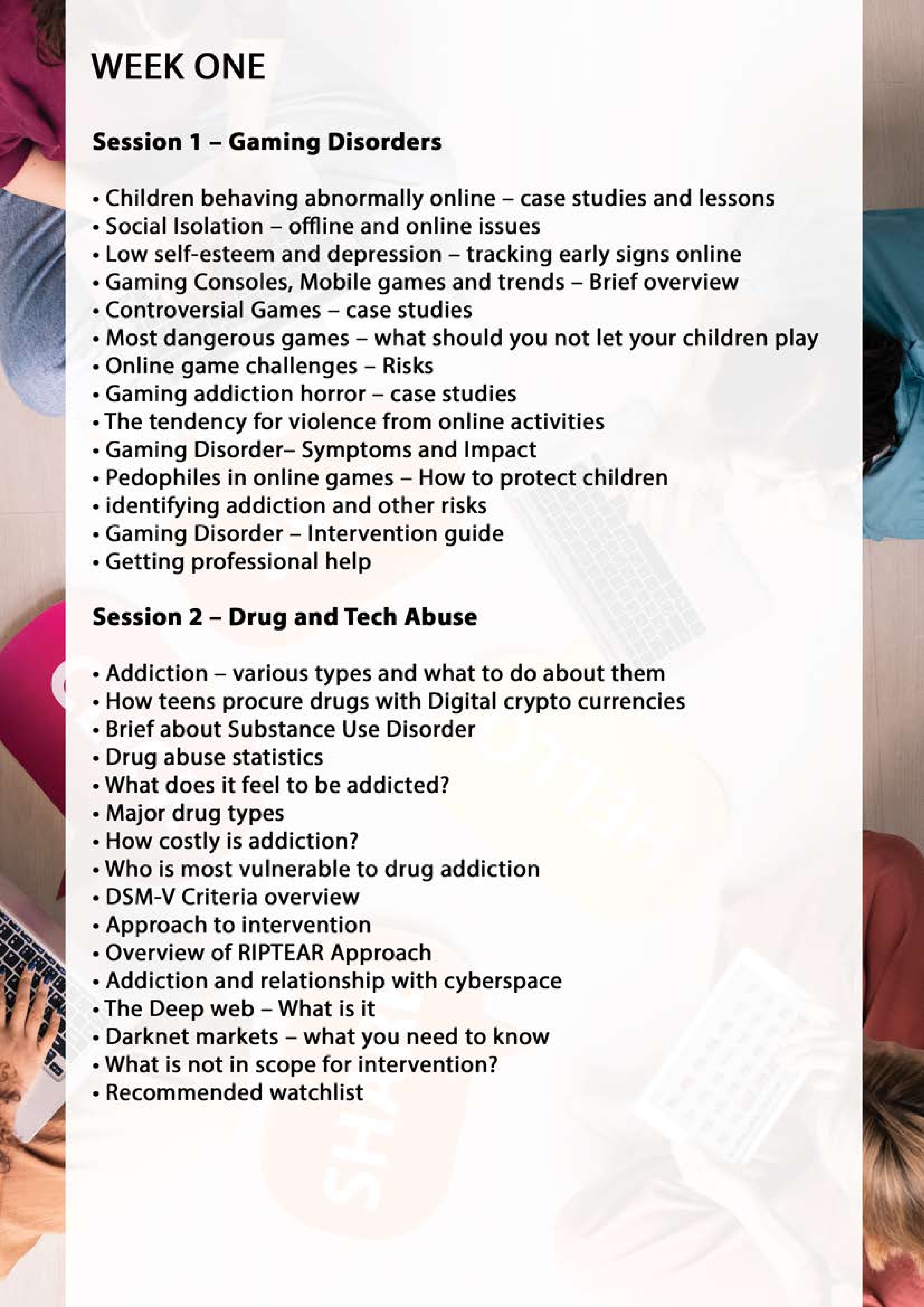
Online Course for Parents, Teachers, Lawyers, Police & Diligent Netizens

Certified Cybercrime Intervention Officer

The program, Cybercrime Intervention Officer, enables the participants to become First Responders.

The First Responders are provided with essential background on cyber psychology and cybercrimes which enables them to detect early signs of problems, especially among school children and teenagers who are the most vulnerable, based on their online activities and behavior.

The program equips the participant with proper guidance for timely and effective intervention, thus reducing the number of cybercrimes and saving the lives of many children from being victims of dangerous crimes such as online blackmail and Sextortion.



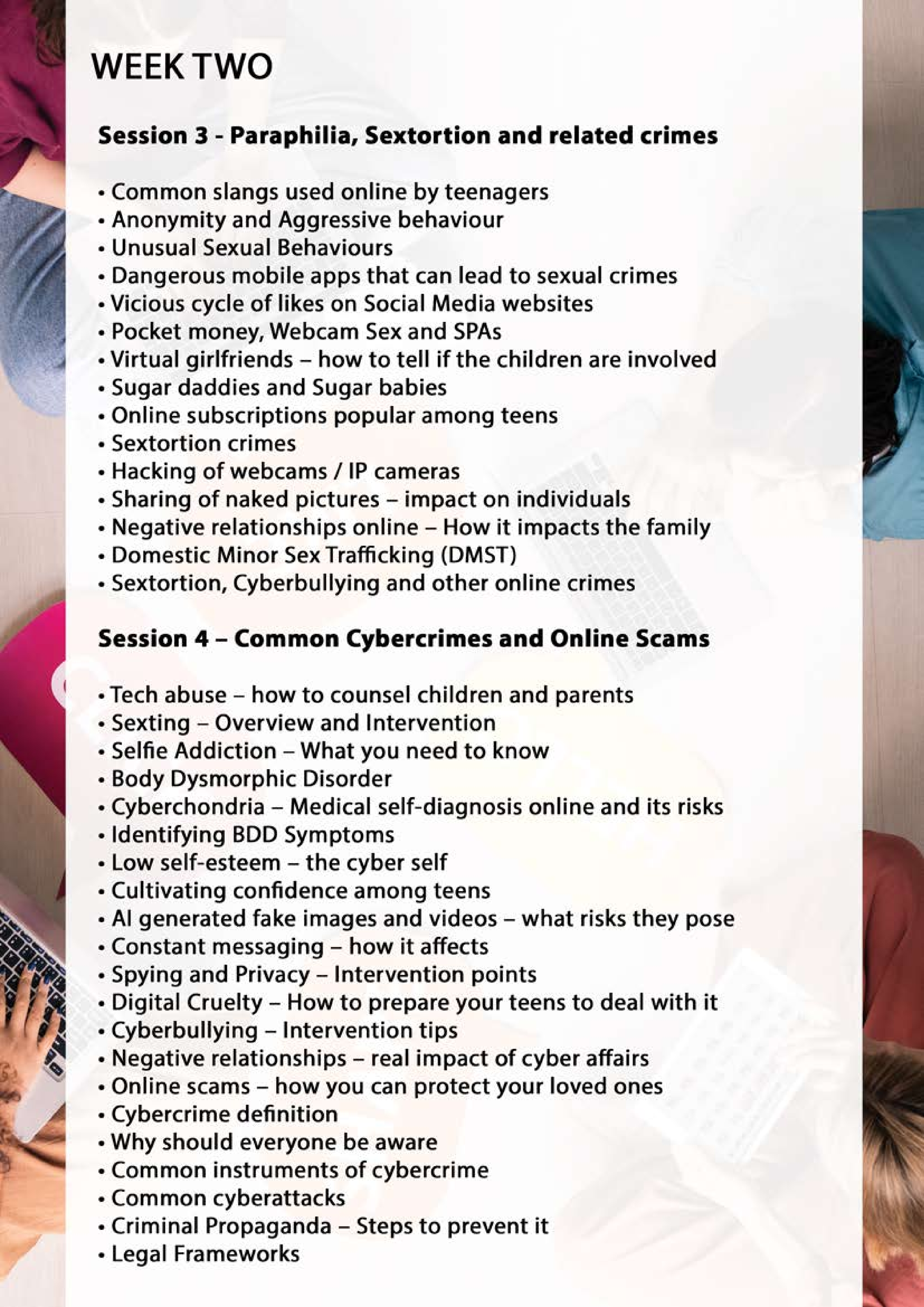
WEEK ONE

Session 1 – Gaming Disorders

- Children behaving abnormally online – case studies and lessons
- Social Isolation – offline and online issues
- Low self-esteem and depression – tracking early signs online
- Gaming Consoles, Mobile games and trends – Brief overview
- Controversial Games – case studies
- Most dangerous games – what should you not let your children play
- Online game challenges – Risks
- Gaming addiction horror – case studies
- The tendency for violence from online activities
- Gaming Disorder– Symptoms and Impact
- Pedophiles in online games – How to protect children
- identifying addiction and other risks
- Gaming Disorder – Intervention guide
- Getting professional help

Session 2 – Drug and Tech Abuse

- Addiction – various types and what to do about them
- How teens procure drugs with Digital crypto currencies
- Brief about Substance Use Disorder
- Drug abuse statistics
- What does it feel to be addicted?
- Major drug types
- How costly is addiction?
- Who is most vulnerable to drug addiction
- DSM-V Criteria overview
- Approach to intervention
- Overview of RIPTEAR Approach
- Addiction and relationship with cyberspace
- The Deep web – What is it
- Darknet markets – what you need to know
- What is not in scope for intervention?
- Recommended watchlist



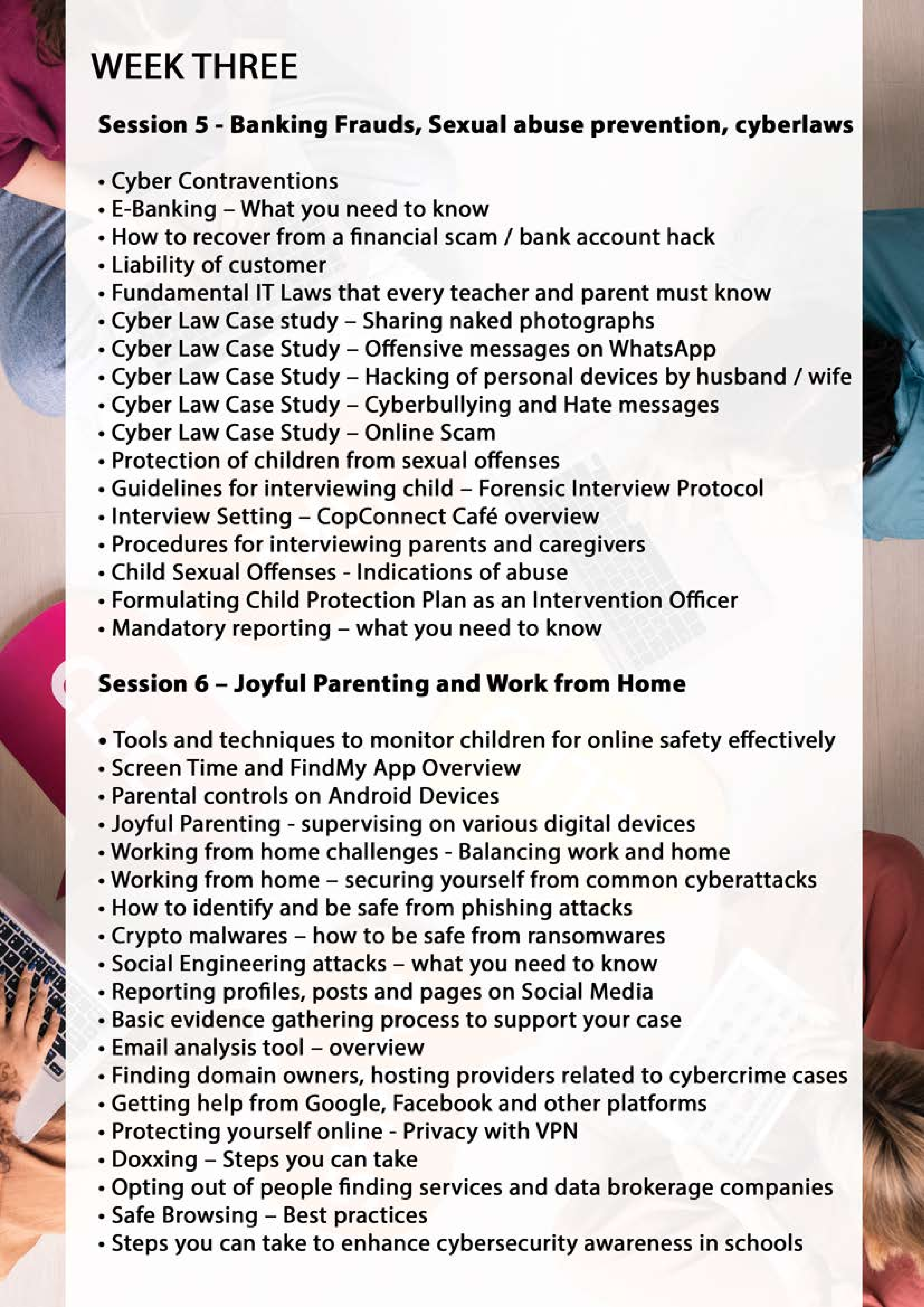
WEEK TWO

Session 3 - Paraphilia, Sextortion and related crimes

- Common slangs used online by teenagers
- Anonymity and Aggressive behaviour
- Unusual Sexual Behaviours
- Dangerous mobile apps that can lead to sexual crimes
- Vicious cycle of likes on Social Media websites
- Pocket money, Webcam Sex and SPAs
- Virtual girlfriends – how to tell if the children are involved
- Sugar daddies and Sugar babies
- Online subscriptions popular among teens
- Sextortion crimes
- Hacking of webcams / IP cameras
- Sharing of naked pictures – impact on individuals
- Negative relationships online – How it impacts the family
- Domestic Minor Sex Trafficking (DMST)
- Sextortion, Cyberbullying and other online crimes

Session 4 – Common Cybercrimes and Online Scams

- Tech abuse – how to counsel children and parents
- Sexting – Overview and Intervention
- Selfie Addiction – What you need to know
- Body Dysmorphic Disorder
- Cyberchondria – Medical self-diagnosis online and its risks
- Identifying BDD Symptoms
- Low self-esteem – the cyber self
- Cultivating confidence among teens
- AI generated fake images and videos – what risks they pose
- Constant messaging – how it affects
- Spying and Privacy – Intervention points
- Digital Cruelty – How to prepare your teens to deal with it
- Cyberbullying – Intervention tips
- Negative relationships – real impact of cyber affairs
- Online scams – how you can protect your loved ones
- Cybercrime definition
- Why should everyone be aware
- Common instruments of cybercrime
- Common cyberattacks
- Criminal Propaganda – Steps to prevent it
- Legal Frameworks



WEEK THREE

Session 5 - Banking Frauds, Sexual abuse prevention, cyberlaws

- Cyber Contraventions
- E-Banking – What you need to know
- How to recover from a financial scam / bank account hack
- Liability of customer
- Fundamental IT Laws that every teacher and parent must know
- Cyber Law Case study – Sharing naked photographs
- Cyber Law Case Study – Offensive messages on WhatsApp
- Cyber Law Case Study – Hacking of personal devices by husband / wife
- Cyber Law Case Study – Cyberbullying and Hate messages
- Cyber Law Case Study – Online Scam
- Protection of children from sexual offenses
- Guidelines for interviewing child – Forensic Interview Protocol
- Interview Setting – CopConnect Café overview
- Procedures for interviewing parents and caregivers
- Child Sexual Offenses - Indications of abuse
- Formulating Child Protection Plan as an Intervention Officer
- Mandatory reporting – what you need to know

Session 6 – Joyful Parenting and Work from Home

- Tools and techniques to monitor children for online safety effectively
- Screen Time and FindMy App Overview
- Parental controls on Android Devices
- Joyful Parenting - supervising on various digital devices
- Working from home challenges - Balancing work and home
- Working from home – securing yourself from common cyberattacks
- How to identify and be safe from phishing attacks
- Crypto malwares – how to be safe from ransomwares
- Social Engineering attacks – what you need to know
- Reporting profiles, posts and pages on Social Media
- Basic evidence gathering process to support your case
- Email analysis tool – overview
- Finding domain owners, hosting providers related to cybercrime cases
- Getting help from Google, Facebook and other platforms
- Protecting yourself online - Privacy with VPN
- Doxxing – Steps you can take
- Opting out of people finding services and data brokerage companies
- Safe Browsing – Best practices
- Steps you can take to enhance cybersecurity awareness in schools

Your Benefits

+ Intervention Officer Certificate
+ Access to exclusive WhatsApp Group
+ Access to class video recordings
+ First Responder ID Card
+ CopConnect Membership

Who Should Attend

The minimum age requirement to attend the CCIO program is 20 years. Admission to the course is subject to application approval. The course is best suited for:

- Parents (Especially Mothers)
- Teachers and Teacher Trainees
- Counselors
- Medical Professionals
- Judicial Officers
- Lawyers and Law students
- Cybersecurity professionals
- Armed Forces Personnel
- Law enforcement officers

Examination

The exam consists of 50 multiple choice questions out of which the candidates need to correctly answer a minimum of 60% questions to clear the exam successfully.

In September 2019 the New York Times noted that in the previous year technology companies reported to the US National Center for Missing and Exploited Children (NCMEC) over 45 million photographs and videos of children being sexually abused. This was more than twice the number reported in the previous year.

64% of Americans don’t know what steps to take in the event of a data breach.

Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes

Information Sharing And Analysis Center
(non-profit)

www.isacindia.org
support@isacindia.org
twitter.com/isacindia
facebook.com/isacindia

+91 8882-560-560