



Parent's Session Manual



CYBER DIVISION, KERALA POLICE

PREFACE

Online sexual exploitation of children has emerged as a global emergency, after the Covid-19 pandemic. A global survey revealed that 54% of young people experienced online sexual harm before turning 18.

In India — the world's second-largest internet user base with over 100% urban penetration — reports of online child abuse have been increasing since 2008, with a major spike during the pandemic.

Smartphone usage among children is widespread, with 83% of 10–14-year-olds using them, and 90% of the population owning more than one internet connection. Extortion, online grooming, live-streaming, and AI-generated child sexual abuse material (CSAM) are on increase. Offenders often gain the trust of victims before threatening and exploiting them, using platforms like online games, messenger apps, and social media.

Emerging AI technologies have introduced new vectors for abuse. Recent law enforcement operations have documented the misuse of deepfake technologies, AI-enabled grooming chatbots, encrypted live-streaming platforms, and Webcam Child Sex Tourism (WCST). These offences, characterised by borderless execution and offender anonymity.

Children today are often exposed to adult content disguised within cartoons and animations. Online grooming takes place through interactive games and private messaging apps. This makes parental awareness and vigilance critical — knowing what children are consuming digitally, what they are doing, and who they are interacting with online.

Parental controls are one of the most effective technical safeguards against online child abuse, social media exploitation, and problematic device use. These tools can filter harmful content, monitor communication channels, and manage screen time. The effectiveness of parental controls is maximised when combined with active parental engagement, open dialogue between parents and children, and comprehensive digital literacy education.

Protecting children online requires urgent, united action from parents, educators, law enforcement, and policymakers. By raising awareness of threats like cyberbullying and grooming, strengthening child protection frameworks, and equipping families with digital safety tools, we can help create a safe and empowering online environment for the next generation.

This book has been developed as a practical resource and reference guide — bridging research, policy insights, and real-world prevention strategies. It aims to empower parents, educators, and professionals with the knowledge and tools necessary to safeguard children in the digital environment, thereby fostering a safe, informed, and resilient next generation.

TABLE OF CONTENT

Module 1: Understanding the Digital World & Child Psychology

Module 2: Building Digital Wellness

Module 3: Online Privacy & Cybersecurity Basics

Module 4: Social Media Risks & Online Threats

Module 5: Reporting & Evidence Collection

Module 6: Parental Controls - Tools & Techniques

Introduction to the Parent's Manual

This manual has been created to support parents in guiding their children through the digital world with confidence and care.

In today's environment, children face increasing risks online—such as exposure to harmful content, cyberbullying, online predators, and digital addiction. Parents are often the first line of defense, yet many feel uncertain about how to manage technology at home. This handbook aims to bridge that gap by offering **practical tools, simple explanations, and family-friendly strategies.**

By learning how to set healthy boundaries, recognize warning signs, and foster open conversations, parents can help children build strong digital habits while also protecting their emotional and physical wellbeing.

The manual provides:

1. Clear explanations of common online risks in simple, non-technical language.
2. Step-by-step guides for using parental controls, privacy settings, and monitoring tools.
3. Conversation starters and role-play activities to build trust and communication.
4. Practical family strategies for balancing screen time with offline life.
5. Resources to extend digital safety practices beyond the home.

This guide is flexible—it can be read cover-to-cover as a complete manual, or used selectively to address specific challenges as they arise.

Purpose and Goals of the Manual

To empower parents with the knowledge and confidence to:

Protect children from online abuse and harmful influences.

Guide safe and respectful use of social media.

Recognize and prevent digital and mobile addiction.

Support children in developing digital resilience, empathy, and critical thinking skills.

Guiding Principles

1. **Child Safety First** – Every tip and tool prioritizes the emotional, physical, and online safety of children.
2. **Empowerment Through Guidance** – Equip parents with practical skills to guide—not just control—their children's digital lives.
3. **Balanced Digital Life** – Encourage a healthy mix of online learning, play, and offline family time.
4. **Partnership & Communication** – Build strong parent-child trust and involve children in co-creating digital rules.
5. **Respect and Empathy** – Model and teach kindness, diversity awareness, and respect for privacy in all digital interactions.

LETTER TO PARENTS

Subject: Keeping Our Children Safe Online – KID GLOVE

Dear Parents/Guardians,

This year, Kerala Police is introducing a comprehensive program to help students build the skills they need to navigate the online world safely. Topics include online child abuse prevention, safe and responsible social media use, and strategies to avoid digital addiction.

The lessons are interactive, age-appropriate, and encourage children to share what they learn with their families. We invite you to participate in reinforcing these lessons at home by discussing the safety tips provided in our take-home materials.

Together, we can create a safer, healthier, and more respectful digital environment for our children.

Sincerely,

Ankit Asokan IPS,
Superintendent of Police,
Cyber Operations,
Cyber Headquarters, PHQ
Thiruvananthapuram

Module Explained in following Template:

1. **Module Title & Theme**
2. **Goals for Students** (what they will be able to do)
3. **Standards Addressed** (if aligning to national or educational standards)
4. **Lesson Overview** (short intro to the topic)
5. **Vocabulary** (key terms for the lesson)
6. **Activities** (step-by-step, numbered activities with materials needed)
7. **Let's Talk** (discussion questions to prompt critical thinking)
8. **Takeaway** (key learning points to remember)
9. **Optional Game / Simulation** (if applicable, online or offline)

Purpose of Parent's Manual

The online world offers children endless opportunities for learning, creativity, and connection. But it also brings risks—cyberbullying, online grooming, sextortion, harmful challenges, and exposure to unsafe content. Many parents feel unsure of how to guide their children through these challenges, especially when technology changes so quickly.

This handbook has been created to empower parents with two key tools:

Psychology – Understanding how children think, feel, and behave online. This is especially important during adolescence, when hormonal and emotional changes shape how children see themselves, respond to peers, and explore their identity. At this stage, they are curious, vulnerable to peer pressure, and sometimes secretive. Building trust and open communication is essential so that children feel safe sharing their online experiences.

Technology – Practical, step-by-step guidance on using parental controls, safety settings, monitoring tools, and digital wellbeing features across devices, apps, and networks.

By combining these two approaches, parents can create a safe and supportive digital environment for children

How to Use this Manual

- **Learn:** Each chapter introduces a common online risk or challenge in **simple, non-technical language**, with real-life examples.
- **Act:** Step-by-step guides help you apply the right **technical tools** (like screen time limits, filters, and privacy settings).
- **Connect:** Practical conversation starters and role-play scenarios help you build **open communication and trust** with your child.

- **Reflect:** “Wrap-up” sections at the end of each topic summarize the key takeaways and offer a **family mantra** for safe online behaviour.
- **Extend:** Optional follow-up activities encourage parents to involve children in co-creating family rules for technology use.

This book is about **guidance, balance, and partnership** between parents and children. By blending psychological insight with digital tools—and by recognising the unique challenges of adolescence—families can work together to create a **safe, respectful, and balanced online space**.

Parents also need to keep in mind that technology is constantly evolving. Just as every parent has learned to use a smartphone without ever attending a formal course, they too can **adopt and adapt new technologies** to protect their children online. This handbook is designed to **empower parents with confidence**, showing that with the right knowledge and tools, they can guide their children safely in the digital world.

What's Inside

Children today are growing up in a world where online and offline life are often indistinguishable.

While the internet offers incredible opportunities for learning, creativity, and connection, it also presents a complex landscape of risks that parents must understand.

Protecting our children online begins with recognizing these diverse threats, which range from the immediate discomfort of **Cyberbullying** to more insidious dangers like **Online Grooming** by predators.

Parents also need to be aware of the terrifying reality of **Sextortion**, where children can be coerced or blackmailed.

Beyond direct threats, children are frequently exposed to **Age-Inappropriate Content**, and can easily fall prey to **Online & Mobile Games – Addictive by Design**, thanks to clever psychological tactics and algorithms.

The pervasive nature of **Social Media Dangers** also poses challenges, alongside the emerging threat of **AI-Enabled Exploitation** and the quiet but serious risk of **Identity Theft**.

By becoming aware of these specific dangers, we can better equip ourselves to guide our children through the digital world safely and responsibly.

Understanding the Digital World & Child Psychology



- 1.1** The online risks faced by children (cyberbullying, grooming, sextortion, harmful trends)
- 1.2** The dopamine loop and how tech companies design addictive experiences
- 1.3** Warning signs of mobile/game addiction
- 1.4** Psychological impact of excessive screen use on children's development
- 1.5** Role of parents as proactive digital mentors, not just monitors

Children today are growing up in a world where online and offline life are often indistinguishable.

While the internet offers incredible opportunities for learning, creativity, and connection, it also presents a complex landscape of risks that parents must understand.

Protecting our children online begins with recognizing these diverse threats, which range from the immediate discomfort of **Cyberbullying** to more insidious dangers like **Online Grooming** by predators.

Parents also need to be aware of the terrifying reality of **Sextortion**, where children can be coerced or blackmailed.

Beyond direct threats, children are frequently exposed to **Age-Inappropriate Content**, and can easily fall prey to **Online & Mobile Games – Addictive by Design**, thanks to clever psychological tactics and algorithms.

The pervasive nature of **Social Media Dangers** also poses challenges, alongside the emerging threat of **AI-Enabled Exploitation** and the quiet but serious risk of **Identity Theft**.

By becoming aware of these specific dangers, we can better equip ourselves to guide our children through the digital world safely and responsibly.

1.1 The online risks faced by children (cyberbullying, grooming, sextortion, harmful trends)

Learning Objectives

By the end of this session, children will be able to:

- Recognize different types of online risks (cyberbullying, grooming, sextortion, harmful trends).
- Identify warning signs of unsafe online behaviour.
- Practice safe responses such as blocking, reporting, or asking a trusted adult for help.
- Build confidence in making safer digital choices.

Key Vocabulary

Introduce these terms in simple, child-friendly language before the activity:

Cyberbullying

When someone uses the internet or phone to hurt, tease, or embarrass another person.

Grooming

When a stranger try to trick a child into trusting them online, often pretending to be a friend.

Sextortion

When someone threatens to share private pictures or information unless the child does what they say.

Harmful Trends / Challenges

Online dares or activities that encourage unsafe or dangerous behaviour.

Block & Report

Tools on social media or games to stop bullies or strangers from contacting you.

Warm-Up / Discussion Prompt

Start with quick, relatable questions:



Has anyone ever seen someone being teased or bullied online in a game or chat?

What would you do if a stranger suddenly sent you a friend request?

Why do you think people join online challenges?



Encourage children to share in a safe, non-judgmental way

Core Activity (Interactive)

Role-Play Scenarios

Divide into small groups. Each group acts out a short scenario (provided by the educator) and shows how to respond safely.

Examples:

- ▶ Receiving a mean message in a group chat.
- ▶ A “new friend” asking for personal photos.
- ▶ Peer pressure to join a risky online challenge.

Guided Discussion

Ask children:

- ▶ “What signs helped you spot something unsafe in the activity?”
- ▶ “How did it feel to act out saying NO or blocking someone?”
- ▶ “What can you do in real life if this happens to you or a friend?”

Don't keep secrets about unsafe messages, always tell a trusted adult

Wrap-Up

**Think Before You Click.
If it feels wrong, it probably is.
Block. Report. Tell a trusted adult.**

Write the mantra on the board or give children a handout with the three steps

Extension / Homework



Reflection Journal

Ask children to write or draw one “red flag” they will watch out for online.

Family Agreement

Create a “Safe Internet Promise” together (e.g., no sharing personal info, always ask before joining new groups)

1.2 Understanding the Dopamine Loop

Learning Objectives

By the end of this session, parents will be able to:

- Understand what dopamine is and how it affects children’s screen use.
- Recognise how tech and gaming companies design apps and games to keep children hooked.
- Identify signs that their child may be “trapped” in a dopamine loop.
- Learn practical strategies to break the cycle and build healthier tech habits.

Key Vocabulary

Variable Rewards (Slot Machine Effect)

Unpredictable rewards — sometimes big, sometimes small, sometimes none — that make people keep trying. Used in loot boxes, spins, or game rewards.

Habit Formation

The process by which repeated actions become automatic over time .
e.g., checking a phone every time it buzzes without thinking.

Streaks & Daily Rewards

Game or app features that reward daily use ("log in 7 days in a row"). Missing a day means losing progress, which pressures kids to return.

Endless Scroll / Auto-play

Design features where new videos, posts, or game levels load automatically, giving no natural stopping point.

Social Validation Loop

The repeated cycle of posting, waiting for likes or comments, feeling a dopamine "hit," then posting again for more approval.

Artificial Scarcity

When apps or games create a false sense of urgency (e.g., "limited-time offer," "only 1 hour left") to push kids to act quickly.

User Experience (UX) Design

The way apps/games are built to influence how people feel and behave from colours and sounds to timing of rewards.

Time Blindness

When children (or adults) lose track of how much time has passed while gaming or scrolling.

Warm-Up / Discussion Prompt

Ask parents:

- "Have you ever lost track of time scrolling on social media or binge-watching a series?"
- "If adults struggle to stop, how much harder is it for children with developing brains?"

Core Activity – The “Slot Machine” Demonstration

- Bring a jar with mixed slips of paper: some say “Reward!” (like candy/sticker) and most say “Try Again.”
- Parents take turns drawing.
- Notice: The unpredictability makes them want to keep trying — just like children with games.
- **Debrief:** This is the same “variable reward system” used by tech companies.

Guided Discussion

- Why children are more vulnerable: Their self-control system is still developing.
- Difference between **healthy engagement** (educational, creative apps) and **designed addiction** (streaks, loot boxes, endless scrolling).
- How parents can shift focus: from punishment (“Stop playing now!”) to awareness (“This game is designed to keep you hooked. Let’s set a timer together”).

Warning Signs Your Child May Be in a Dopamine Loop

- Difficulty stopping once they start.
- Irritability when devices are taken away.
- Loss of interest in offline hobbies.
- “Time blindness” — not realising hours have passed.
- Obsession with rewards (skins, badges, likes).

Wrap-Up – Parent’s Mantra



Extension / Homework for Parents

Teach Kids About “The Hook”

Explain that the game is designed to keep them playing, not because it’s “too fun to stop,” but because it’s programmed to feel that way.

Break the Loop

Set tech-free times (before bed, during meals).

Encourage hobbies that also trigger dopamine — sports, arts, music.

Choose Games & Apps Wisely

Prefer ones with clear end points, without endless scrolling or streak pressure.

1.3 Warning Signs of Mobile/Game Addiction in Children

Learning Objectives

By the end of this session, parents will be able to:

- Identify behavioural, physical, emotional, and social warning signs of possible mobile/game addiction.
- Differentiate between healthy gaming and problematic gaming habits.
- Reflect on their own child's tech use and recognize red flags early.
- Take initial, practical steps to restore balance before the problem worsens.

Key Vocabulary

Addiction – When someone cannot control how much they use something, even when it causes harm.

Compulsion – A strong, hard-to-control urge to do something (like checking a game repeatedly).

Withdrawal Signs – Emotional changes (anger, sadness, restlessness) when the device/game is taken away.

Escapism – Using games or screens to avoid problems or difficult feelings.

Balance – Healthy use of technology where screen time doesn't harm sleep, study, relationships, or health.

Warm-Up / Discussion Prompt

Ask parents:



What's the longest your child has ever played a mobile game without a break? How did they react when you asked them to stop?

Scenario prompt: "Imagine your child says they'll play for just 10 minutes, but an hour later they're still gaming. How would you handle it?"



(Allow parents to share experiences and feelings)

Core Activity – Red Flag Sorting Game

Objective: Help parents distinguish between normal gaming enthusiasm and warning signs of addiction.

Step 1: Provide flashcards with behaviours (mix of healthy and unhealthy). Examples:

- Excitedly tells you about a game level.
- Refuses to eat dinner until game is finished.
- Plays 30 minutes after homework, then stops.
- Lies about how long they've been playing.
- Stays up until 2 AM gaming on school nights.
- Plays an hour, then goes outside to cycle.

Step 2: Parents sort them into two baskets:

- **Healthy Interest**
- **Warning Sign of Addiction**

Step 3: Facilitator reviews and clarifies why certain behaviours cross into "red flag" territory.

Guided Discussion

Lead parents to reflect:

- “Why do children get hooked so easily on games?”
(link to dopamine/reward loop in simple terms).
- “How do you tell the difference between passion (interest) and problem (addiction)?”
- “What small steps can you take if you notice multiple

Wrap-Up

Main takeaways for parents

- **One or two signs** may be normal enthusiasm, but **many signs together, over time, mean risk of addiction.**
- Watch for **changes in sleep, school, mood, and family interaction.**
- **Parents' mantra:**
“Games are fun, but balance is the rule. If screens take over life, it's time to act.”

Extension / Homework



Addiction grows silently. If you notice multiple signs appearing together over weeks or months, it's time to set structured limits and have an open, non-judgmental conversation with your child.

1.4 Psychological Impact of Excessive Screen Use on Children

Learning Objectives

By the end of this session, parents will be able to:

- Recognize the emotional and psychological effects of excessive screen use (e.g., irritability, anxiety, mood swings).
- Understand how screens affect children's self-esteem, focus, and relationships.
- Identify early signs of emotional strain caused by overuse.
- Develop practical steps to restore balance and protect children's mental well-being.

Key Vocabulary

Anxiety – A feeling of worry or nervousness, sometimes linked to online pressures (likes, followers, gaming success).

Mood Swings – Quick changes in emotions (happy one moment, angry or sad the next).

Sleep Disruption – Trouble falling or staying asleep due to late-night device use.

FOMO (Fear of Missing Out) – The anxiety of feeling left out when others are online, gaming, or posting on social media.

Self-Esteem – How a child feels about themselves, which can be affected by comparisons online.

Digital Overload – Mental tiredness caused by too much screen exposure.

Warm-Up / Discussion Prompt

Ask parents:

"Have you noticed your child becoming cranky, moody, or restless after long screen sessions?"

Scenario: "Imagine a child who stays up late gaming and struggles to wake up for school. How might this affect their mood, focus, and relationships the next day?"

Core Activity – Emotion Mapping Exercise

Objective: Help parents connect screen habits to children's emotions and behaviours.

Step 1: Provide a worksheet with two columns:

- “After Screen Time”
- “After Outdoor/Offline Play”

Step 2: Parents brainstorm what emotions/behaviours they observe in each situation.

Examples:

- After screen time → irritable, restless, withdrawn, hyperactive.
- After outdoor play → calm, cheerful, talkative, energetic in a healthy way.

Step 3: Group shares findings to highlight contrasts.

Guided Discussion

Lead parents in reflecting:

- “Why do you think excessive screen time often leads to irritability or anxiety?” (Introduce dopamine loop & overstimulation in simple language.)
- “How does poor sleep from late-night screen use affect a child's mood and school performance?”
- “What can parents do to replace screen time with healthier emotional outlets (like sports, art, or family bonding)?”

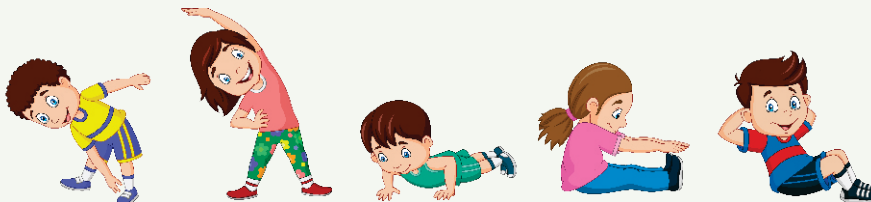
Wrap-Up

Main Takeaways:

- Too much screen time doesn't just affect physical health — it impacts children's **emotions, sleep, relationships, and self-esteem**.
- Balanced screen use = better mood, focus, and family connection.
- **Parent's mantra:**
“Screens affect feelings. Less screen, more peace.”

Extension / Homework

Set limits, ensure screen-free sleep, encourage outdoor play



1.5 Role of parents as proactive digital mentors, not just monitors

Learning Objectives

By the end of this session, parents will be able to:

1. Understand the difference between being a “monitor” (only policing) vs. a “mentor” (guiding, teaching, supporting).
2. Recognize why open conversations and shared digital experiences build trust.
3. Learn practical ways to co-explore online spaces with children.
4. Develop strategies to move from control-based rules to guidance-based mentorship.

Key Vocabulary

Monitor – A parent who only checks or restricts device use (rules without conversation).

Mentor – A parent who guides children, teaches safe choices, and models healthy digital behaviour.

Digital Citizenship – Teaching children how to be safe, responsible, and respectful online.

Trust Bridge – Building open communication so children feel safe sharing their online experiences.

Co-Use – Parents exploring apps, games, or websites alongside children, creating teachable moments.

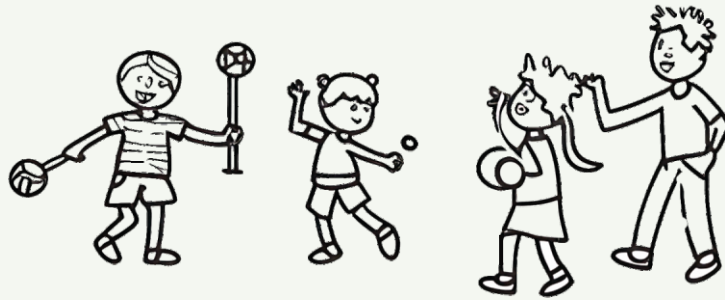
Proactive Guidance – Setting boundaries while also teaching skills for safe, independent digital use.

Warm-Up / Discussion Prompt

Ask parents:

- “When your child asks about a new app or game, is your first instinct to say No or to sit with them and explore together?”
- Scenario: A 12-year-old installs a social media app without permission. The parent has two choices: scold and delete, or ask the child to show how the app works and talk about risks. Which response do you think builds more trust for the future?

Core Activity - “Monitor vs. Mentor” Role-Play



Step 1: Divide parents into small groups. Give each group a scenario card:

- Child asks to download a popular gaming app.
- Child receives a friend request from someone unknown.
- Child wants to watch a YouTube challenge trend.

Step 2: Each group acts out two responses:

1. **Monitor Role** – Parent just says “No” or enforces a strict rule.
2. **Mentor Role** – Parent sits with the child, explores together, explains risks, and guides safe choices.

Step 3: After role-play, groups discuss: Which approach encourages honesty and better long-term behaviour?

Guided Discussion

Questions for parents:

- “How does being a mentor change the way children see your guidance?”
- “What risks might children hide if parents only monitor without mentoring?”
- “What simple steps can parents take to mentor—without needing advanced tech knowledge?”

Examples:

- Ask children to teach you about a game/app.
- Watch YouTube together and talk about ads, clickbait, or safe content.
- Share your own online mistakes or learnings to model openness.

Wrap-Up

Main Takeaways for Parents:

- Monitoring alone may lead to secrecy; mentorship builds **trust + safety**.
- Parents don't need to know everything about tech—they need to stay curious, involved, and approachable.
- **Parent's Mantra:**
“Not just a monitor, but a mentor – guiding my child to be safe and wise online.”

Extension / Homework

Instead of: “You've been playing that game too long. Turn it off now!”

Try: **“I see you've been playing for an hour. Let's take a break — want to help me cook dinner or go for a walk?”**

Instead of: Secretly checking your child's phone,

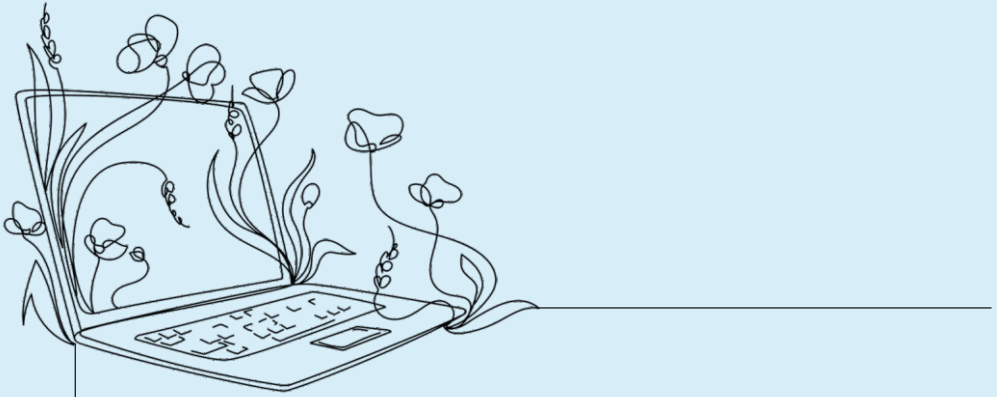
Try: **“Let's review your friend list together — we can make sure they're all people you know in real life.”**

Note

Note



Building Digital Wellness



- 2.1** **Setting healthy tech boundaries early**
- 2.2** **Internationally recommended screen time limits (WHO, AAP, NIMHANS)**
- 2.3** **Creating device-free zones and family tech rules**
- 2.4** **Modelling healthy device habits as parents**
- 2.5** **Recognizing risky online trends and challenges**

Welcome to a chapter dedicated to a fundamental aspect of raising children in the digital age: digital wellness.

It's about ensuring that technology serves as a positive and balanced part of their life, rather than becoming a source of stress or unhealthy habits.

Just as a healthy diet and regular exercise are vital for a child's physical growth, mindful technology use is crucial for their mental and emotional development.

This chapter will provide you with the tools and insights to help your child build a healthy relationship with screens from a young age.

Here's a roadmap of what we will cover:

- **Setting Healthy Tech Boundaries Early:** Learn how to introduce technology with clear rules and expectations from the start, laying a foundation that will guide your child's habits as they grow.
- **Internationally Recommended Screen Time Limits:** We'll break down the official recommendations from global health organizations like the World Health Organization (WHO), the American Academy of Paediatrics (AAP), and India's NIMHANS, providing a clear framework for age-appropriate screen time.
- **Creating Device-Free Zones and Family Tech Rules:** Discover how to establish physical spaces and times in your home where technology is put away, encouraging face-to-face interaction and other non-digital activities.
- **Modelling Healthy Device Habits as Parents:** Understand the power of your own example. We'll explore how you can be a role model for balanced tech use, because your habits speak louder than your words.
- **Recognizing Risky Online Trends and Challenges:** Learn how to spot and talk to your child about dangerous social media trends and viral challenges, ensuring they have the awareness to avoid potentially harmful situations.

2.1 Setting Healthy Tech Boundaries Early

Learning Objectives

By the end of this session, parents will:

- Understand why early rules and routines about technology matter for children.
- Learn how to set age-appropriate screen time limits and device-free zones at home.
- Be able to create a family agreement on technology use.
- Feel confident in guiding children to balance screen time with offline activities.

Key Vocabulary

Screen Time – The amount of time spent using a device like a phone, tablet, or computer.

Digital Balance – Mixing online activities with offline ones like play, study, or hobbies.

Device-Free Zone – Areas in the home where phones or gadgets are not allowed (like the dining table or bedroom).

Boundaries – Family rules that keep technology use safe and healthy.

Warm-Up / Discussion Prompt

Ask parents to reflect and share:



- "How much time does your child spend on devices each day?"
- "What happens when you ask your child to put the phone/tablet away?"
- "Think of one moment this week where tech interrupted family time – what could have been different?"

Real-life scenario prompt:

A child refuses to come to dinner because they are in the middle of an online game. How would you handle this?

Core Activity

Role Play: Two Voices

Scenarios (choose one):

A 10 year old refuses to stop gaming at bedtime.

A teen brings a phone to the dining table.

A 7 year old gets upset when cartoons are turned off.

Activity Steps:

Round A – Command & Control (2 min): **Parent gives the classic “Because I said so” response.**

Round B – Family Values Framing (2 min): **Parent sets the same rule but explains why** (“We all need rest to feel good tomorrow, so devices sleep outside bedrooms”).

Reflect (8 min): Groups compare — Which voice reduced conflict? Which voice helps children learn self control and empathy?

Guided Discussion

Facilitator leads reflection:

- Why do children resist limits? (addiction, fun, peer pressure)
- How do consistent rules make children feel safe?
- Share success stories: Parents who created “no phone at dining table” rules report more family conversations and bonding.

Prompt: “What is one tech rule you want to try at home starting today?”

Wrap-Up

Boundaries today, balance tomorrow.

- Small daily rules add up to big, lifelong habits.
- Setting limits is not punishment – it is protection.
- Children follow what they see: be the role model.

Extension / Homework

Device-Free Challenge: Choose one evening in the week where the whole family avoids screens and instead does a fun activity (games, walk, storytelling). Reflect together after.

2.2 Internationally Recommended Screen Time Limits

Internationally Recommended Screen Time Limits

The core message from all three organizations is consistent: the goal is not to eliminate screens, but to ensure they are used in a way that supports, rather than hinders, a child's healthy development. This involves balancing digital engagement with essential real-world activities like physical play, social interaction, and sleep.



1. Under 2 Years (WHO & AAP)

- **No screen time** (except video calls with family).
- Babies learn best from **real-world interaction** – talking, singing, and playing with parents.

2. Ages 2–5 Years (WHO & AAP)

- Up to **1 hour per day**, only **high-quality content**, ideally co-viewed with a parent.
- Example: An educational cartoon watched together is better than random videos.

3. Ages 6–12 Years (AAP & NIMHANS)

- **1–2 hours of recreational screen time per day** (not including school/learning).
- Balance with **outdoor play, family time, and hobbies**.
- Encourage tech use for **learning, creativity, and connection**, not just passive scrolling.

4. Teenagers (13–18 Years)

- No fixed “hours” – instead, focus on **balance**.
- Ensure screen use doesn't interfere with:
 - Sleep
 - School work
 - Physical activity
 - In-person social connections
- Teach them to **self-regulate** and take **screen breaks**.

Learning Objectives

By the end of this session, parents will:

- Identify age-appropriate screen time limits recommended by global health experts.
- Distinguish between recreational and educational screen time.
- Draft or update their own customized Family Media Plan.

Key Vocabulary

Introduce and explain these words simply:

Recreational screen time: Screens for fun (games, cartoons, social media)—not schoolwork.

Educational screen time: Screens for learning (classes, homework).

Family Media Plan: Family agreement on when, where, and how devices are used.

Screen hygiene: Habits that keep tech use healthy, like breaks and no screens before bed.

Warm-Up / Discussion Prompt



Ask

“How much recreational screen time do you think is healthy for kids of different ages?”

Core Activity

Parents respond to Questions:

- "How is screen use different for each of my kids?"
- "What routines or tech-free times work for us?"
- "What feels hardest to change?"

Guided Discussion

Lead a parent reflection:

Where does quality improve screen use? (co-viewing, creative apps, video calls with relatives, coding — not just passive watching)

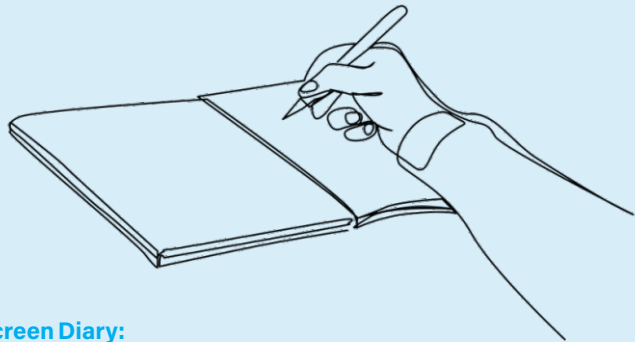
What are the warning signs for too much screen time? (lost sleep, skipped homework, irritability, less physical activity)

Why do experts separate time for fun vs. time for schoolwork?

Wrap-Up

The best guideline is balance—physical activity, family time, sleep, and school work should all fit in the day.

Extension / Homework



Family Screen Diary:

Track each family member's recreational and educational screen time for 3 days.

Hold a family meeting to discuss:

Which routines are working?

Where can we make one healthy change?

Update your Family Media Plan: set/review rules for bedtime, weekends, and device-free zones.

2.3 Creating Device-Free Zones & Family Tech Rules

Learning Objectives

By the end of this session, parents will:

- Recognize the importance of having “tech-free” times and spaces at home.
- Work with children to create simple family rules for healthy technology use.
- Encourage positive offline activities to balance screen time.

Key Vocabulary

Device-Free Zone – A place in the home where gadgets (mobiles, tablets, laptops, TVs) are not allowed.

Tech Curfew – A set time when all devices must be turned off.

Digital Balance – Healthy use of technology alongside offline activities (family time, play, rest).

Screen-Free Time – Specific moments of the day (meals, bedtime, study time) with no screens allowed.

Warm-Up / Discussion Prompt

Start with a relatable question:

- “Has your child ever been on their phone during dinner?”
- “How do you feel when everyone is sitting together, but each person is on a separate screen?”

Scenario: Imagine a family where the father is watching TV, the mother is scrolling social media, and the child is gaming. They are all in the same room but not talking. What's missing here?

Core Activity



Activity 1: "Design a Tech-Free Zone"

- Parents (in groups) sketch a map of a typical home (kitchen, bedroom, living room).
- Together, they decide which areas should be device-free zones (e.g., dining table, bedroom).
- Each group explains why they chose those spaces.

Activity 2: "Family Tech Rules Role-Play"

- Divide into pairs: one acts as the parent, the other as the child.
- Practice setting a simple rule (e.g., "No phones after 9 PM" or "No devices during dinner").
- Switch roles to see both perspectives.

Guided Discussion

Lead with reflection questions:

- "Why do you think mealtimes or bedtime should be device-free?"
- "How can parents make sure rules apply to everyone, not just children?"
- "What offline activities could replace screen time in device-free zones?"

Encourage parents to share real-life struggles (e.g., children resisting rules, parents struggling to model behaviour) and brainstorm solutions together.

Wrap-Up

Summary Points:

- Agree on device-free zones (bedrooms, dining table).
- Set a tech curfew (no devices after a set time).
- Lead by example – children follow what they see.
- Replace screen time with bonding activities: board games, walks, storytelling.

Extension / Homework

- **Family Task:** Sit together and create a “Family Tech Agreement.”
 - **Decide 2 device-free zones** and **1 daily screen-free time** (like dinner).
 - Write rules on a chart and display it at home.

2.4 Modelling Healthy Device Habits as Parents

Learning Objectives

By the end of this session, parents will:

- Understand that children learn digital habits by watching their parents.
- Commit to small, realistic changes that show children balanced technology use.

Key Vocabulary

Digital Role Model – A person whose technology use influences others (especially children).

Phubbing – Ignoring someone in front of you because you are focused on your phone.

Screen-Time Awareness – Being mindful of how much time is spent on devices.

Tech-Life Balance – Managing screen time alongside work, family, and personal well-being.

Warm-Up / Discussion Prompt

Ask parents

- “Have you ever told your child to get off the phone while you were scrolling on your own?”
- “What message do children get if parents use devices at the dining table or bedtime?”

Scenario: A child asks their mother something at dinner. She replies, 'Just a minute' while still on WhatsApp. The child stops asking and quietly eats. What does the child learn from this situation?

Core Activity

Activity : Mirror Reflection

- Give parents cards with common “unhealthy habits” written on them (e.g., checking phone while driving, staying up late online, replying to work emails at dinner).
- Ask: “If your child copied this habit, how would it affect them?”
- Parents share reflections.

Guided Discussion

Facilitator leads reflection:

- “Do children listen more to what we say or what we do?”
- “What small device habits can parents change today that will set a strong example?”
- “How can parents balance work demands with family time without sending mixed messages to kids?”

Encourage parents to share personal struggles and strategies, such as leaving phones outside the bedroom, using “Do Not Disturb” mode, or keeping phones aside during meals.

Wrap-Up

Key Mantra:

"Children follow what we do,
not what we say."

Summary Points:

- Parents are the first digital role models.
- Kids copy not only screen rules but also parents' digital habits.
- Replacing small unhealthy habits (late-night scrolling, phubbing) with healthy ones sets a strong example.
- Family tech values should be lived, not just spoken.

Extension / Homework

Family Activity: Instead of evening screen time, try one offline bonding activity (board game, storytelling, evening walk).

2.5 Recognizing Risky Online Trends & Challenges

Learning Objectives

By the end of this session, parents will:



- Understand what online "trends" and "challenges" are and why children may be drawn to them.
- Recognize common warning signs of dangerous online challenges.
- Guide children to think critically before joining viral trends.

Key Vocabulary

Online Trend – A popular activity, dance, meme, or idea that spreads quickly on the internet.

Online Challenge – A task or dare shared online, often encouraging others to copy and post their version.

Viral Content – Posts, videos, or memes that spread very quickly across social media.

Peer Pressure (Digital) – Feeling pushed to take part in online activities because “everyone else is doing it.”

Digital Red Flags – Warning signs that a trend or challenge may be harmful (e.g., promoting risky behaviour, secrecy, physical danger).

Warm-Up / Discussion Prompt

Ask parents

- “Have you ever heard your child mention a viral challenge or trend you didn't understand?”
- “Why do you think children join these challenges even if they seem silly or unsafe?”

Scenario: A 12-year-old sees friends posting a dangerous “dare challenge” online. He feels left out because he hasn't tried it yet. What might he do? How could a parent guide him here?

Core Activity

Activity : “Safe or Risky?”

- Facilitator shares a mix of imaginary online trends (some safe, some risky). Example:
 - o Dance routine challenge (safe)
 - o Eat spicy food in 30 seconds (risky)
 - o Donate toys and post about it (safe)
 - o Choking challenge (dangerous)
- Parents work in groups to label each as **Safe / Risky / Dangerous** and explain why.

Guided Discussion

Facilitator leads reflection:

- “What makes children so tempted to try these challenges?” (peer approval, curiosity, fear of missing out)
- “How can parents stay aware of what's trending online without spying?”
- “What phrases can parents use to keep communication open when kids bring up online challenges?”

Encourage parents to share personal experiences of hearing about trends too late, and brainstorm proactive strategies (like checking trending sections, asking kids casually, or discussing news stories).

Wrap-Up



**“Not every trend is a friend –
think before you click or join.”**

Summary Points:

- Many online challenges are harmless fun, but some can be risky or life-threatening.
- Peer pressure online is real; children may join trends to “fit in.”
- Parents should talk with children, not at them, about online challenges.
- Teaching kids to ask, “Could this hurt me or others?” builds critical judgment.

Extension / Homework

Ongoing Habit: Once a week, ask children casually, “What's trending among your friends online this week?” – to keep communication open.

Note

Online Privacy & Cybersecurity Basics



- 3.1 Strong passwords & use of password managers**
- 3.2 Privacy settings across major platforms (Facebook, YouTube, Instagram)**
- 3.3 Identifying phishing, scams, and malware**
- 3.4 Safe browsing habits and content filters**

3.1 Strong passwords & use of password managers

Introduction: This module helps parents understand the importance of creating strong, unique passwords and introduces them to the practical benefits of using a password manager.

Learning Objectives

By the end of this session, parents will:

- Explain why a strong, unique password is a critical first line of defense against online threats.
- Identify the key components of a strong password (length, complexity, and uniqueness).
- Understand the risks associated with using weak passwords or reusing the same password across multiple sites.
- Recognize the benefits of using a password manager to securely store and generate complex passwords.

Key Vocabulary



Password: A secret word or phrase used to log in to a website or account. Think of it as the key to a digital door.

Hacker: A person who tries to gain unauthorized access to computer systems or accounts.

Password Manager: A secure digital vault that stores all your passwords for you, so you only have to remember one master password.

Two-Factor Authentication (2FA): An extra layer of security. Even if a hacker gets your password, they can't get into your account without a second thing, like a code sent to your phone.

Warm-Up / Discussion Prompt



- **Scenario:** "Imagine you have a single key that opens your front door, your car door, your bank safe, and your bicycle lock. What happens if you lose that one key?"
- **Relate to Passwords:** "This is similar to using the same password for all your online accounts—your email, social media, online banking, and gaming platforms. If a hacker gets that one password, they can get into everything. This is called 'password reuse,' and it's one of the most common ways people get hacked."

Core Activity: The "Password Strength Test" Challenge

Objective: To demonstrate the difference between a weak and a strong password in a hands-on, non-technical way.



Use the website:

<https://www.security.org/how-secure-is-my-password>

Guided Discussion: From Theory to Practice

After the activity, bring the groups back together and lead a discussion using the following questions:

- "What did this activity teach you about the difference between a weak and a strong password?"
- A password manager is like a high-tech security guard that remembers all the keys for you. You only have to remember one master key to get into the vault."

Wrap-Up

Summary Points:

- o **Length is Power:** The longer the password, the harder it is to guess. Aim for 12 characters or more.
- o **Mix it Up:** Combine letters (upper and lowercase), numbers, and symbols.
- o **Be Unique:** Never reuse a password. One password, one account.
- o **Trust a Manager:** Use a password manager to securely store and generate complex passwords for you.

Mantra

**One password, one account.
Let the password manager do the work.**

Extension / Homework

Parents create one **family password rule chart** (e.g., "Never reuse, use passphrases, enable 2FA").

Install a trusted password manager (e.g., Bitwarden, 1Password, or built-in options like Google/Apple Keychain) and set it up together.

3.2 Privacy settings across major platforms (Facebook, YouTube, Instagram)

Privacy settings on major platforms are crucial for protecting personal information and controlling online presence. They allow users to manage who sees their data, limit exposure to cyber threats, and maintain a sense of control over their digital footprint. By understanding and utilizing these settings, individuals can mitigate risks associated with data breaches, identity theft

Learning Objectives

By the end of this session, parents will:

1. Understand why privacy settings matter for children's safety online.
2. Identify key privacy features in commonly used apps (YouTube, Instagram, WhatsApp).
3. Apply step-by-step settings to protect their child's profile, location, and personal data.
4. Teach children to review privacy settings regularly as part of healthy digital habits.

Key Vocabulary

Privacy Settings – Controls that let you decide who can see your posts, profile, or activity.

Public vs Private Account – Public = anyone can see your content; Private = only approved friends can.

Two-Factor Authentication (2FA) – Extra security step that requires a code in addition to your password.

Blocking & Reporting – Tools to stop strangers or bullies from contacting your child.

Location Sharing – A feature that can reveal your child's real-world location to others if not disabled.

Warm-Up / Discussion Prompt

Ask parents

"If your child posts a photo on Instagram, who do you think can see it — friends only, or strangers too?"

"Have you ever checked if your child's YouTube watch history and recommendations are safe?"

10



Activity 1: The Privacy Check-up Tour

What to do:

1. Log in together to the Facebook account you want to check.
2. Navigate to Settings & Privacy > Settings.
3. Click on the Privacy Checkup tool. This will walk you through five key areas:

- ★ Who can see what you share: Review who can see future posts, past posts, and your friends list.
- ★ How to keep your account secure: Check the password and turn on two-factor authentication?
- ★ How people can find you on Facebook: Adjust who can send friend requests and look you up using your email or phone number.
- ★ Your data settings on Facebook: Review which apps and websites have access to your Facebook account.
- ★ Your ad preferences: See what information Facebook uses to show you ads.

Activity 2: The "View As" Exercise

This activity helps visualize how the account looks to different people and reinforces the importance of setting your audience.

Steps:

1. Go to the account's profile page.
2. Click on the three dots (...) under the profile name and select View As.
3. This will show you what your profile looks like to a complete stranger (someone who is not a friend on Facebook).
4. Then, use the search bar at the top of the page to type in the name of a specific friend and see what they can view.

Activity 3: The "Tagging and Timeline" Audit

This focuses on settings that control how others can interact with the account.

What to do:

1. Navigate to Settings & Privacy > Settings > Profile and Tagging.
2. Review the settings with your child, focusing on these questions:
 - ★ Viewing and Sharing: "Who can post on your profile?" and "Who can see what others post on your profile?"
 - ★ Tagging: "Who can see posts you're tagged in on your profile?" and "When you're tagged in a post, who do you want to add to the audience of the post if they aren't already in it?"
 - ★ Reviewing: "Review posts friends tag you in before they appear on your profile?" and "Review tags people add to your posts before the tags appear on Facebook?"
3. Enable the review settings for tagging and posts to ensure that nothing appears on the timeline without permission.

Guided Discussion

Facilitator reflection:

- "Why do many children prefer public accounts? How can parents explain the risks without sounding controlling?"
- "What could happen if location sharing is left ON?"
- "How often should families sit together to review privacy settings?"

Wrap-Up-Mantra

"Privacy is protection.
Settings today = safety tomorrow."

Extension / Homework

- **Practical Task:** Parents sit with their child and review privacy settings on Instagram, Facebook etc.
- **Discussion at Home:** Ask the child:
 - o “Who do you really want to see your posts?”
 - o “How would you feel if a stranger saw your photos or messaged you?”
- **Two-Factor Authentication (2FA).**

3.3 Identifying Phishing, Scams, and Malware

Learning Objectives

By the end of this session, parents will:

1. Recognize common signs of phishing emails, scam messages, and fake websites.
2. Understand how malware can sneak into devices through unsafe downloads or links.
3. Teach children simple “stop-and-think” steps before clicking or sharing information.

Key Vocabulary

Phishing – Fake messages/emails that try to steal personal information (like passwords or bank details).

Scam – A trick designed to cheat people, often by promising rewards or pretending to be someone trustworthy.

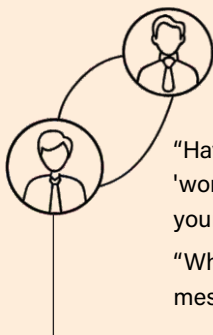
Malware – Harmful software that can damage devices, steal data, or spy on users.

Clickbait – Misleading links or headlines designed to get people to click without thinking.

Suspicious Link – A web link that looks strange (misspelled words, odd endings) and may lead to unsafe sites.

Warm-Up / Discussion Prompt

Ask parents



"Have you ever received a message saying you 'won a prize' or asking you to click a link to verify your bank account?"

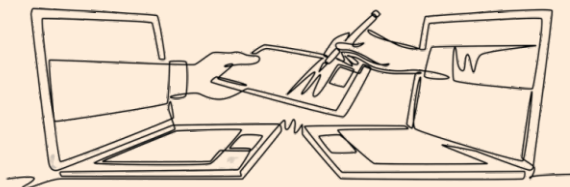
"What do you usually do when you get such messages?"

Core Activity – Spot the Scam Challenge

Activity name: "Real or Fake?"

Show parents printed or projected examples of:

- o A real bank SMS vs a fake phishing SMS.
- o A genuine email from a school vs a scam "scholarship" email.
- o An app download from Google Play vs a suspicious APK link.



Guided Discussion

Facilitate reflection:

- "Why do scammers target children with 'free skins, coins, or rewards' offers?"
- "How can parents explain to kids that clicking unknown links is like opening a stranger's door at home?"
- "What's the best family rule when a child receives a suspicious message or link?"

Wrap-Up - Mantra

"Think before you click. If it feels wrong,
it's wrong."

Extension / Homework

Digital Hygiene: Parents install/update antivirus or parental controls on family devices

3.4 Safe browsing habits and content filters

Learning Objectives

By the end of this session, parents will:

1. Explain what safe browsing means and why it matters for children.
2. Recognize the role of content filters in blocking harmful or age-inappropriate material.
3. Teach children simple browsing "do's and don'ts."
4. Set up family-friendly browsing environments at home.

Key Vocabulary



Safe Browsing – Using the internet carefully to avoid harmful or unsafe websites.

Content Filter – A tool that blocks inappropriate websites, videos, or searches.

Pop-up – A small window that suddenly appears on a website, often with ads or scams.

Search Settings – Options in Google, YouTube, or browsers that help hide unsafe content.

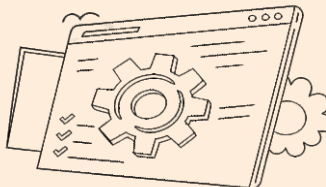
Whitelist / Blacklist – A list of approved (safe) or blocked (unsafe) websites.

Warm-Up / Discussion Prompt

Ask parents

- “When your child searches for cartoons, have you ever worried about what else might pop up?”
- “Have you or your child ever clicked something by mistake and ended up on the wrong website?”

Core Activity- Safe or Unsafe Browsing?



Facilitator demonstrates enabling **Google SafeSearch, YouTube Restricted mode.**

Google SafeSearch (Web Browsing)

SafeSearch helps hide explicit images, videos, and websites from Google search results.

On a Computer (Browser)

1. Go to **Google Search Settings**.
2. Under **Safe Search Filters**, check the box “**Turn on Safe Search.**”
3. Scroll down and click **Save**.
4. Optional: Click **Lock SafeSearch** (requires a Google account login). This prevents kids from turning it off.

YouTube Restricted Mode

Restricted Mode filters out potentially mature content on YouTube.

On a Computer (Browser)

1. Go to **YouTube.com** and log in.
 2. At the top right, click your **Profile Picture**.
 3. Scroll down to **Restricted Mode**.
 4. Toggle **Activate Restricted Mode** → ON.
- (Optional) Click **Lock Restricted Mode on this browser** (requires login)

Guided Discussion

Prompts for reflection:

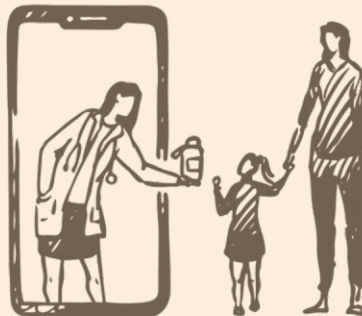
- "What risks do children face when they accidentally land on unsafe sites (ads, scams, inappropriate content)?"
- "Why is relying only on supervision not enough, and why are filters a useful backup?"
- "How can families balance trust with protection while letting kids explore online?"



Wrap-Up - Parent's Mantra

**"Smart clicks + Safe filters
= Safer kids online."**

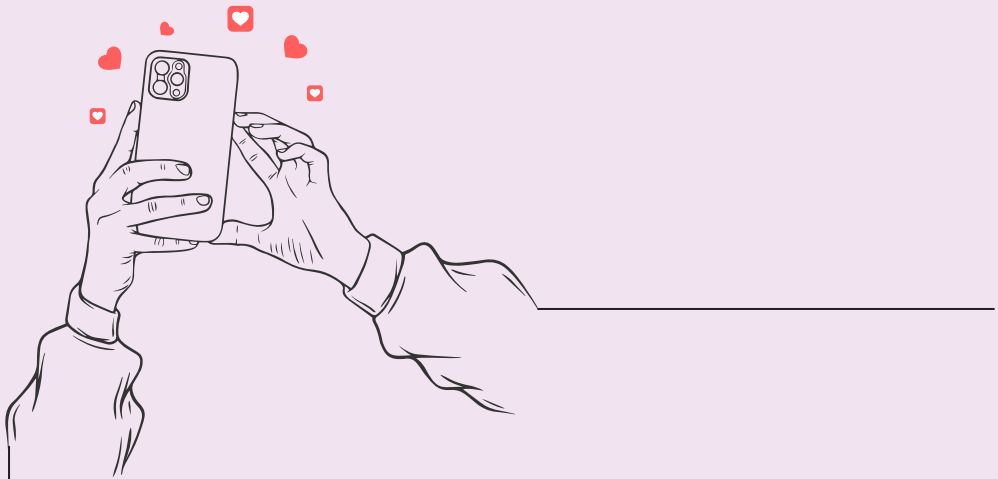
Extension / Homework



Family Browser Check-Up: Parents set up safe search and parental controls on devices at home.

Note

Social Media Risks & Online Threats



- 4.1** Detecting cyberbullying, grooming, and sextortion
- 4.2** Stranger danger and fake identities
- 4.3** Recognizing manipulative online conversations
- 4.4** Preventing oversharing of personal information

Welcome to a chapter that tackles the more serious and complex dangers of the digital world. While the internet is a place of connection and learning, it's also home to hidden risks that can affect your child's safety and well-being.

This section is designed to help you become a vigilant and informed guide, capable of recognizing and responding to threats that go beyond simple technical issues.

Think of social media as a public park: it's full of opportunities for fun and friendships, but it also requires awareness of who is around and what they're doing.

This chapter will equip you with the knowledge to recognize the "red flags" and navigate these risks alongside your child.

Here's a roadmap of what we will cover:

- **Detecting Cyberbullying, Grooming, and Sextortion:** Learn how to identify the subtle and overt signs of these dangerous online behaviours. We'll provide you with the tools to recognize when a child is being targeted and what to do about it.
- **Stranger Danger and Fake Identities:** We'll explore how to identify fake online profiles and communicate with your child about the critical rule of not trusting online strangers.
- **Recognizing Manipulative Online Conversations:** Understand the psychological tactics used by predators and manipulators. We'll show you how to spot a conversation that's designed to build trust for a harmful purpose.
- **Preventing Oversharing of Personal Information:** Learn why sharing too much online can be a major risk. We'll provide practical strategies to help your child protect their personal information, from their location to their daily routines.

4.1 Detecting cyberbullying, grooming, and sextortion

Learning Objectives

By the end of this session, parents will:

- Recognize early warning signs of cyberbullying, grooming, and sextortion in their child's online activity or behaviour.
- Understand the tactics used by online abusers and bullies.
- Support children in reporting incidents safely without fear or shame.

Key Vocabulary



- **Cyberbullying** – Repeated use of technology to harass, threaten, or embarrass someone.
- **Grooming** – When someone builds trust with a child online to exploit or harm them.
- **Sextortion** – Threatening to share private/intimate images unless demands are met.
- **Red Flags** – Warning signs of unsafe online behaviour or manipulative conversations.
- **Trusted Adult** – A parent, teacher, or caregiver a child can turn to when feeling unsafe online

Warm-Up / Discussion Prompt

- Ask: "If your child came home with a bruise, you'd notice. But what if their hurt is online? How would you spot it?"

- Share short real-life scenarios:

1. A child suddenly avoids using their phone or deletes apps.

2. A teen spends long hours online, but becomes secretive about chats.

3. A student is unusually anxious before school because of online rumours.

Invite parents to guess what these could signal (cyberbullying, grooming, or sextortion).

Core Activity-Role-Play & Scenario Card

Activity: "Name the Risk"

- Educator presents different scripted chat messages or scenarios.
- Parents identify whether it's **cyberbullying, grooming, or sextortion**, and raise a corresponding card (e.g., red = sextortion, yellow = grooming, blue = cyberbullying).

Examples:

1. "You're ugly, no one likes you. Just quit the group." →

Cyberbullying

2. "You're so mature for your age, let's keep our chats private

from your parents." → **Grooming**

3. "Send me a private photo or I'll share the screenshot I

already have." → **Sextortion**

4. "Haha, everyone at school is laughing at you, check

Instagram." → **Cyberbullying**

5. "I can buy you game credits if you just video call me alone

tonight." → **Grooming**

Guided Discussion

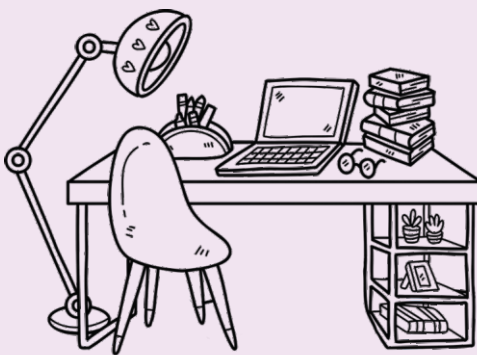
- **Cyberbullying:** Why children often don't report (fear of losing device, embarrassment).
- **Grooming:** How predators build trust over weeks/months before asking for inappropriate things.
- **Sextortion:** How threats escalate quickly, and why children may panic and comply.
- Stress that **early detection and open communication** are key.

Wrap-Up

Takeaways

- **Notice the Signs:** Changes in mood, secrecy, or sudden fear of going online are signals.
- **Don't Blame, Support:** Children should never feel it's their fault.
- **Stop – Save – Report:** Stop engaging, Save evidence, Report to platform/authorities.

Extension / Homework



1. **Practical Task:** Explore together how to report/block on the child's most-used app or game.
2. **Conversation Starter:** Parents ask their child, "If someone made you uncomfortable online, how would you like me to respond?" and agree on a safe plan.

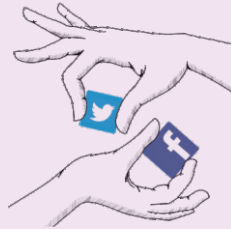
4.2 Stranger danger and fake identities

Learning Objectives

By the end of this session, parents will:

- Recognize that strangers online can pretend to be friends, classmates, or trusted people.
- Identify **red flags** of fake identities (e.g., limited profile info, avoiding video calls, too much flattery).
- Teach children safe responses to suspicious friend requests or chats.
- Encourage children to check with parents before accepting new connections online.

Key Vocabulary



Stranger (online) – Someone you do not personally know in real life, even if they “seem” friendly online.

Fake Identity / Catfishing – Pretending to be someone else online using false photos, names, or details.

Impersonation – Using another person's profile or pictures to trick others.

Red Flag – A warning sign that something may be unsafe or untrue.

Block/Report – Tools to stop strangers or fakes from contacting your child.

Warm-Up / Discussion Prompt

- **Ask:** “Would you let your child walk away with a stranger who says, ‘I know your friend’s name?’”
- **Relate this to online behaviour:** Just because someone knows small details (like school name or favourite game), it doesn't mean they are safe.
- **Share a real-life case (simplified):** A child was messaged by someone pretending to be a classmate, but it turned out to be an adult using stolen photos.

Core Activity- Interactive Game: Real or Fake?

Game:

- Show parents sample online profiles or chat screenshots (mock examples, not real). Some are genuine, others contain suspicious signs.
- Parents raise a **Green Card** (Real) or **Red Card** (Fake/Stranger Danger).
- Discuss why they chose that answer.

Examples:

1. Profile picture looks too perfect / like a celebrity photo → Red Flag
2. Someone refuses to video call but insists on chatting privately → Red Flag
3. A known school friend who you've met offline → Green (Safe)
4. A gamer with no profile details but asking for personal info → Red Flag

Guided Discussion

- Why is it easy to create fake profiles online?
- Why do children sometimes trust strangers more quickly online?
- How can parents teach children to double-check before accepting requests?
- Reinforce that it's okay to say no and involve parents immediately.

Wrap-Up

Takeaways:

Not everyone online is who they say they are.
Don't talk, don't share, don't meet strangers online.
Block + Report instead of replying.
When in doubt, check it out with a trusted adult.

Extension / Homework

1. Parent and child review the child's friend list together and remove people they don't know offline.
2. Parent asks child, "If someone online says they know me but you've never met them, what would you do?" Practice safe responses.

4.3 Recognizing Manipulative Online Conversations

Learning Objectives

By the end of this session, parents will:

- Understand how online predators or scammers use flattery, pressure, or false promises to manipulate children.
- Spot red flags in digital conversations (asking for secrets, pushing for personal info, creating urgency, guilt-tripping).
- Equip children with safe responses to stop manipulation.
- Build open communication at home so children feel safe reporting suspicious chats.

Key Vocabulary

Manipulation – When someone tries to trick or control you for their own benefit.

Flattery – Excessive compliments used to lower a child's guard ("You're the smartest kid I know").

Guilt-tripping – Making someone feel bad if they don't do what the other person wants ("If you don't share a photo, I'll be sad").

Red Flags – Warning signs that a conversation may not be safe.

Boundaries – Personal limits about what you share and with whom.

Gaslighting – Making someone doubt what they know or remember.

Emotional Blackmail – Using threats or guilt to make someone do what they want.

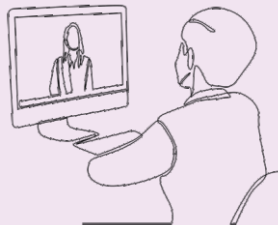
Boundaries – Limits you set to keep yourself safe and comfortable.

Warm-Up / Discussion Prompt

Ask parents

"If a salesperson promised your child a free toy just for giving their name and phone number, would you allow it?" Then compare it with online "free offers" or strangers asking for info.

Core Activity - Raise Red-Flag Hunt



Instructions for Educator:

- Read aloud different sample chat lines (one by one).
- After each line, pause and ask parents:
"Is this safe or a red flag?"
"Why do you think so?"
- Encourage parents to raise a Red Flag Card (or simply say "Red Flag") when they hear manipulative or unsafe language.

Sample Chat Lines:

1. "You're so mature for your age, I can tell you're special." → Flattery – Red Flag
2. "Don't tell your parents, they won't understand." → Secrecy – Red Flag
3. "If you don't send me a picture, I'll stop being your friend." → Pressure/Guilt-Tripping – Red Flag
4. "I can get you free game coins, just give me your email." → False Promise/Scam – Red Flag

Debrief:

After each response, explain why it's unsafe and how manipulators use such tactics.

Guided Discussion

- What made these conversations manipulative?
- How do manipulators make children feel (special, guilty, scared, pressured)?
- Why do children sometimes hesitate to tell parents about these chats?
- Emphasize: **It's not the child's fault** if someone tries to manipulate them online. The responsibility lies with the manipulator.

Wrap-Up

Takeaways for Children:

- If someone online asks you to **hide, hurry, or feel guilty**—that's a red flag.
- **Stop - Block - Tell:** Stop the chat, Block the person, Tell a trusted adult.
- Real friends respect your boundaries.

Extension / Homework

Encourage parents to have a chat with children about their online friends and to recognize any changes in behaviour that may signal manipulation.

4.4 Preventing oversharing of personal information

Learning Objectives

By the end of this session, parents will:

- Understand what counts as **personal information** (beyond just names and phone numbers).
- Recognize how oversharing (photos, school name, location tags) can put children at risk.
- Teach children to pause and think before posting or sharing online.
- Establish clear family rules about sharing safely on social media, messaging apps, and games.

Key Vocabulary

Personal Information – Details like name, age, address, school, phone number, photos, passwords.

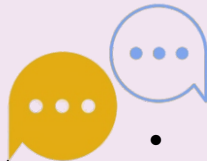
Digital Footprint – The trail of information you leave online through posts, comments, and photos.

Oversharing – Sharing too much information online that could reveal private details.

Privacy Settings – Tools that control who can see your posts and personal details.

Stranger Access – When people you don't know can see what your child posts.

Warm-Up / Discussion Prompt



- Ask: "If your child wore a T-shirt with their name, age, and school printed on it and walked in a crowded market, would you be comfortable? How is that similar to what children sometimes post online?"
- Share a real-life example: A teen posted a photo in their school uniform with a visible badge. Strangers could now know where they study.

Core Activity - Hands-On Game: "Share or Don't Share?"

Activity:

- Educator shows different slides with examples of posts:
 1. A birthday cake with the child's full name on it.
 2. A selfie with friends in a park (no location tag).
 3. A story showing the child's home address.
 4. A group photo at school sports day (school name visible).
 5. A vacation picture with no personal details.

- Parents raise a Green Card (Safe to Share) or Red Card (Not Safe to Share).
- Short discussion follows each example.

Guided Discussion

- What makes some posts safe while others risky?
- How small details (like a background sign or location tag) can reveal big information.
- Why children may not realize that “only friends” online can still screenshot and share.
- Educate Children: Once posted, information is hard to take back.

Wrap-Up

Takeaways

- **Think Before You Share.**
- **Personal = Private-** Don't post details that reveal who you are, where you live, or where you'll be.
- **Check Settings + Ask First-** Always check privacy controls and ask a trusted adult before posting.

Extension / Homework



1. **Digital Footprint Map:** Parent asks child to list all places they've shared personal details online (social media, gaming usernames, comments).
2. Together, decide which ones are safe and which need to be deleted/hidden.

Note

Reporting & Evidence Collection



5.1 How to report to official helplines:

- i. **1098 - Child Helpline**
- ii. **1930 - Cyber Financial Fraud Helpline**
- iii. **cybercrime.gov.in - National Cybercrime Reporting Portal**

5.2 How to collect admissible evidence: screenshots, URLs, timestamps

5.3 Reporting on social media platforms directly

Welcome to the most proactive and empowering chapter of this handbook. While the previous sections focused on prevention, this chapter is about action.

When an online threat or incident occurs, knowing what to do immediately is the difference between a problem and a solution.

This section will guide you through the crucial process of reporting online harm and collecting the necessary evidence to ensure a swift and effective response.

Think of it as preparing a digital emergency kit. Just as you have a first-aid kit at home for physical injuries, this chapter will show you how to be prepared for digital incidents. We'll provide clear, step-by-step instructions on how to use official resources and social media platforms to report a problem, as well as how to gather the right kind of evidence that can be used by authorities.

Here's a roadmap of what we will cover:

- **How to Report to Official Helplines:** We'll demystify the process of using India's key helplines and portals. You'll learn the specific purpose of 1098 (Child Helpline), 1930 (Cyber Financial Fraud Helpline), and the National Cybercrime Reporting Portal (cybercrime.gov.in) so you know exactly who to call in an emergency.
- **How to Collect Admissible Evidence:** Learn why a simple screenshot isn't always enough. We'll teach you how to capture admissible evidence by including critical details like URLs and timestamps, which are essential for any official report.
- **Reporting on Social Media Platforms Directly:** Discover how to use the built-in reporting tools on your child's favourite apps. We'll show you how to formally report harmful content or a suspicious account directly to the platform, making the internet a safer place for everyone.

5.1 How to report to official helplines 1098 | 1930 | cybercrime.gov.in

Learning Objectives

By the end of this session, parents will:

- Identify the correct helpline or portal to use for different online threats and emergencies.
- Teach children and family members that **reporting is safe, free, and confidential**.
- Build confidence in using official channels rather than ignoring or hiding incidents.

Key Vocabulary



1098 - Childline: A 24x7 toll-free helpline for children in distress (abuse, neglect, bullying, grooming).

1930 - Cyber Financial Fraud Helpline: Emergency number to report online banking fraud, UPI scams, or digital payment theft immediately.

cybercrime.gov.in - National Cybercrime Reporting Portal: Official Government of India portal for reporting cybercrime, online harassment, sextortion, fraud, and child exploitation.

Report: Informing authorities about an unsafe or illegal situation.

Confidential: Information is kept private and used only to provide help.

Warm-Up / Discussion Prompt

- Ask: "If your child fell and broke a leg, you'd call an ambulance. But what if your child is bullied online, scammed in a game, or harassed on social media — who would you call?"

- Share short scenarios:
 1. A stranger asks a child for photos online.
 2. A parent loses money after clicking a fake bank link.
 3. A teen is threatened with a private video being leaked.
- Ask parents: "Which helpline or portal would you use in each case?"

Core Activity - Interactive Simulation: Match the Helpline



Activity:

- Educator presents **scenario cards** (realistic but age-appropriate).
- Parents say the correct reporting channel: **1098, 1930, or cybercrime.gov.in.**

Examples:

1. A child receives threatening DMs from a stranger asking to keep secrets. → **1098 / cybercrime.gov.in**
2. Your bank account is debited after a fake UPI request. → **1930**
3. Someone creates a fake Instagram account of your child and shares edited photos. → **cybercrime.gov.in**
4. A child calls saying their friend is being beaten at home and afraid to tell anyone. → **1098**
5. Teen is blackmailed to pay money or else private images will be posted. → **cybercrime.gov.in + police**

Guided Discussion

- Why do families sometimes hesitate to report (fear, shame, “maybe it will stop on its own”)?
- Why quick reporting makes a difference (e.g., 1930 works best if reported within hours of fraud).
- Emphasize: **Children are never in trouble for reporting — the problem is with the criminal, not the child.**
- Parents should model confidence: “If something happens, we report, not hide.”

Wrap-Up

Takeaways

- **1098 – For children in distress.**
- **1930 – For online financial fraud.**
- **cybercrime.gov.in – For all other cybercrimes (harassment, sextortion, fake accounts, fraud).**
- **Stop – Call – Report.**

Extension / Homework

1. **Family Emergency Card:** Parents and children create a small card with important numbers:
 - o 1098 (Childline)
 - o 1930 (Cyber Fraud Helpline)
 - o Local Police (100/112)
 - o cybercrime.gov.in (written clearly)
2. **Practice Drill:** Each family member practices saying what they would report and to whom.

5.2 How to collect admissible evidence

Screenshots | URLs | Timestamps

Learning Objectives

By the end of this session, parents will:

- Understand why digital evidence is important when reporting cybercrimes.
- Learn how to capture and store screenshots, links (URLs), and timestamps correctly.
- Avoid mistakes that make evidence invalid (editing, deleting, or ignoring).
- Teach their children the importance of **“saving proof /evidence”**

Key Vocabulary

Evidence: Information that can prove what happened.

Screenshot: A digital picture of what is visible on the screen.

URL (Web Address): The exact online link where harmful content is found.

Timestamp: The date and time of the incident, automatically saved on devices or platforms.

Admissible: Accepted by law or police as valid proof.

Metadata: Hidden details in files that show when and where they were created.

Warm-Up / Discussion Prompt



- Ask parents: “If someone bullies your child in the school playground, what would you do to prove it?” (e.g., eyewitnesses, CCTV, photos).
- Then ask: “What about online bullying or fraud? How can we prove it?”
- Share a short story: A child deletes a threatening message out of fear. Later, when the parent wants to report, there's no proof. → Ask: What could the child have done instead?

Core Activity - Hands-On Practice: "Save the Proof/Evidence"

Step 1 – Demonstration by Educator:

- Show how to take a screenshot on a phone or computer.
- Point out that the **screenshot must show the username, message, and time in the same frame.**
- Show how to copy the **URL** of a webpage or fake profile.
- Highlight the importance of recording the **date and time** (take a photo of device clock if needed).

Step 2 – Parent Practice Exercise:

- Give each group of parents a **printed scenario** card (e.g., "You receive a scam email," "Your child gets a threatening chat message").
- Task: Practice **writing down the steps** they would take to preserve evidence:
 1. Take a screenshot.
 2. Copy and save the URL.
 3. Note the timestamp (date/time).
 4. Store safely (folder, pen drive, or email to self).

Guided Discussion

- Why is it important **not to edit or crop** screenshots?
- Why should we **note the date and time immediately**?
- How can parents encourage children to **"pause and save proof"** instead of reacting in panic?
- Connect to real life: "Just like we keep receipts for purchases, we keep digital receipts for online incidents."

Wrap-Up

3
S

- **See – Save – Share** → If something wrong happens online:
 1. **See** the harmful message/content.
 2. **Save** with screenshot + URL + timestamp.
 3. **Share** with helplines (1098 / 1930) or cybercrime.gov.in.
- Never delete proof instead save it
- Evidence protects your child and helps police take action.

Extension / Homework

Parents practice with children how to take screenshots on their devices and save URLs.

5.3 Reporting on social media platforms directly

Learning Objectives

By the end of this session, parents will:

- Recognize that most social media apps have **in-built reporting tools**.
- Learn how to **report abuse, fake accounts, cyberbullying, or inappropriate content** on popular platforms.
- Guide children to **report safely** instead of ignoring or reacting emotionally.
- Understand the difference between **blocking, reporting, and unfollowing/muting**.

Key Vocabulary



Report: Telling the platform about harmful or rule-breaking content so it can be reviewed/removed.

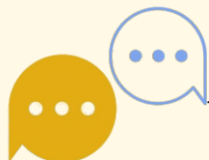
Block: Preventing a user from contacting or seeing your profile.

Mute/Unfollow: Stopping updates from someone without them knowing.

Community Guidelines: Rules set by the platform about what is allowed or not allowed.

Flag: Marking a post, comment, or account as harmful.

Warm-Up / Discussion Prompt



- Ask: "If someone misbehaves in a public park, whom do you complain to?" (Answer: Park security, authority).
- Follow-up: "Similarly, if someone misbehaves on social media, who should we tell first?" → The platform itself.
- Short scenario: A child receives a rude comment on Instagram. What should they do? Delete, reply angrily, ignore, or report?

Core Activity - Hands-On / Role-Play



Step 1 - Demonstration

- Educator shows (via screenshots or a live demo) how to report on:
 - o **Instagram:** Tap three dots → Report → choose reason.
 - o **YouTube:** Flag icon → Report content.
 - o **WhatsApp:** Open chat → More → Report → Block.
 - o **Facebook:** Three dots on post/profile → Find Support or Report

Guided Discussion

- Why is it important for children to **report**?
- What's the difference between **blocking** and **reporting**?
- How can parents reassure children that reporting is not "complaining" but "protecting"?
- Encourage the idea that reporting makes social media safer for everyone, not just your child.

Wrap-Up

- **Don't React – Report!**
- Steps to follow: See → **Report** → **Block** → **Tell Parent**.
- Platforms act faster when harmful content is reported by multiple users.
- Reporting is the child's **first line of defence**, followed by official helplines if needed.

Extension / Homework

- Parents and children spend 15 minutes practicing how to report/block on the apps they use most.
- Parents create a simple chart at home listing steps for reporting on Facebook, Instagram, YouTube, WhatsApp, etc.
- Encourage children to show parents one thing they've reported (even a spam message), so they practice without fear.

Note

Parental Controls – Tools & Techniques



6.1 OS-based tools:

6.1.a Google Family Link

6.1.b Apple Screen Time

6.1.c Microsoft Family Safety

6.2 App-level controls: YouTube Kids, WhatsApp, Instagram

6.3 Network-level controls (DNS filters, router settings)

6.4 Browser-based tools and safe search options

Welcome to a chapter that puts the power of online safety directly into your hands. While open communication is the foundation of a healthy digital relationship, technology provides an essential safety net.

This section is your guide to the world of parental controls—the practical tools and techniques that allow you to manage and filter your child's online experience.

Think of parental controls as the digital equivalent of a seatbelt and a car seat: they're not a substitute for teaching your child safe driving habits, but they provide crucial protection against unexpected dangers.

This chapter will demystify the various types of controls available to you, from the settings built into your devices to the filters that protect your entire home network.

Here's a roadmap of what we will cover:

- **OS-Based Tools:** We'll walk you through the core parental control features of the major operating systems. You'll learn how to use Google Family Link, Apple Screen Time, and Microsoft Family Safety to set screen time limits, approve apps, and filter content across your child's devices.
- **App-Level Controls:** Discover how to use the built-in safety features on popular apps like YouTube Kids, WhatsApp, and Instagram. You'll learn how to lock down privacy settings, manage who your child can communicate with, and control the content they see.
- **Network-Level Controls:** We'll explain the powerful concept of filtering content at the source. You'll learn how to use DNS filters and your router settings to block entire categories of websites, ensuring all devices on your home Wi-Fi network are protected.
- **Browser-Based Tools and Safe Search Options:** Find out how to use the safety features within web browsers themselves. We'll show you how to enable SafeSearch and other browser-based tools that prevent inappropriate search results and content from appearing.

6.1 Operating System based Parental Controls

Learning Objectives

By the end of this session, parents will:

- Understand the purpose of **built-in parental control** tools in operating systems.
- Set **age-appropriate restrictions** on apps, games, and web content.
- Monitor **screen time and device usage** to promote healthy digital habits.
- Use parental controls to **support, not just restrict**, children's online activity.

Key Vocabulary

Parental Control: Built-in tools that help manage what children can access on devices.

Screen Time: Total time spent using a device or specific apps.

Content Filtering: Restricting apps, games, or websites that are inappropriate.

App Approval/Request: Child requests access to an app or game, which parent can approve or deny.

Location Sharing: Ability to see a child's device location for safety.

Activity Reports: Summaries of a child's device usage, apps used, and online activity.

Warm-Up / Discussion Prompt

- Ask: "How do you currently know how much time your child spends on devices or what apps they use?"
- Scenario discussion: "Your child spends hours on games at night and struggles to wake up for school. How could parental controls help?"
- Invite parents to share challenges they face in balancing online safety and independence for their children.

Core Activity - Hands-On / Simulation

Demonstration:

- Show screenshots or live demo of **OS-based parental controls** on:
 - o **Google Family Link** (Android)
 - o **Apple Screen Time** (iOS/Mac)
 - o **Microsoft Family Safety** (Windows/PC/Xbox)

6.1.a Google Family Link



Step-by-step guide for setting up and using Google Family Link on Android for parents:

Step 1 - Install the App

- On your phone, open **Google Play Store** → search **Family Link (for parents)** → Install & Open.

Step 2 - Create/Link Child Account

- If child has a Google account → select **Yes**.
- If not → **Create account** (enter name, DOB, etc.).
- Follow prompts for consent (may ask for card verification).

Step 3 - Connect Parent & Child Devices

- On parent's phone: **Family Link** → **Add Child** → **Link account**.
- On child's device: install **Family Link for children & teens** → sign in with child's Google account.
- Approve connection on parent's phone.

Step 4 – Set Controls

- Open child's profile:
 - o **Screen Time** → set daily limit.
 - o **Bedtime** → set device lock hours.
 - o **App Management** → approve/block apps.
 - o **Content Filters** → restrict apps/games/movies by age.

Step 5 – Monitor Activity

- **App Activity** → see usage & reports.
- Review trends and talk with your child about balance.

Step 6 – Location (Optional)

- Enable **Location Sharing** to see your child's device on a map.

Step 7 – Notifications

- Get alerts when child requests apps.
- Approve or deny instantly.

6.1.b Apple Screen Time



Step 1 – Turn On Screen Time

- Settings → Screen Time → Turn On → **This is My Child's iPhone/iPad.**

Step 2 – Set a Passcode

- Add a 4-digit **Screen Time Passcode** (prevents changes).

Step 3 – App Limits

- Screen Time → **App Limits** → choose categories (e.g., Games) → set daily time.

Step 4 – Downtime

- Screen Time → **Downtime** → set start & end times (only allowed apps)

work).

Step 5 – Content & Privacy

- Turn on **Content & Privacy Restrictions** → manage apps, purchases, explicit content, and web filters.

Step 6 – App & Communication Requests

- Enable **Ask to Buy** for downloads.
- Limit calls/messages during downtime.

Step 7 – Monitor Activity

- **See All Activity** → view usage reports → discuss habits with your child.

Step 8 – Family Sharing (Optional)

- Manage Screen Time remotely via **Family Sharing**.
- Track location with **Find My**.

6.1.c Microsoft Family Safety



Step 1 – Install / Access

- Download **Microsoft Family Safety** (Google Play / App Store / Microsoft Store) or go to **family.microsoft.com**.
- Sign in with your **Microsoft parent account**.

Step 2 – Add Child

- **Add Family Member** → **Child** → enter child's email (or create one).
- Child accepts invite to join your family group.

Step 3 – Screen Time

- Open child's profile → **Screen Time** → set daily/weekly limits for devices, apps, and games.

Step 4 – Content Restrictions

- **Content Filters** → block inappropriate sites, apps, and games by age rating.

Step 5 – Monitor Activity

- **Activity Reports** → see time spent, apps used, websites visited.
- Review weekly with your child.

Step 6 – Location (Optional)

- Enable **location tracking** → see child's device on a map.
- Set alerts for arrivals/departures.

Step 7 – Notifications

- Get alerts when child requests screen time or tries blocked apps/sites.
- Approve or deny instantly.

Guided Discussion

- Why is it important to **explain limits** to children instead of just enforcing them?
- How do parental controls **teach self-regulation** instead of only restricting access?
- Discuss **pros and cons** of different OS tools and device compatibility.
- Encourage parents to **review activity reports weekly** and start conversations based on them.

Wrap-Up



- **Monitor – Guide – Empower:** Tools are there to guide children, not punish them.
- **Set Limits, Encourage Discussion:** Explain why limits exist.
- **Consistency Matters:** Apply limits across devices for balanced digital habits.

Extension / Homework

Parents explore the parental control settings on a child's device and set one screen time limit or content restriction.

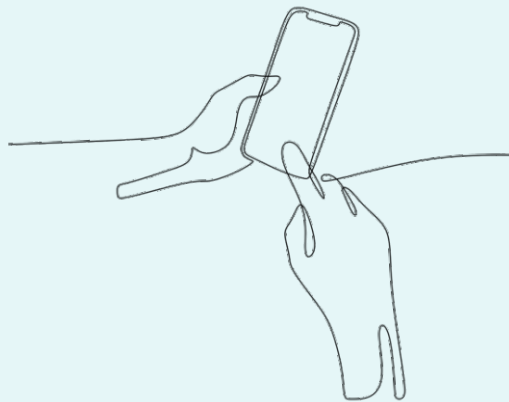
6.2 App Level Parental Controls

Learning Objectives

By the end of this session, parents will:

- Understand the importance of controlling **individual apps** rather than just overall device usage.
- Learn how to **set app-specific limits, privacy settings, and content restrictions.**
- Guide children to use apps **safely and responsibly.**
- Recognize apps that may be inappropriate, addictive, or risky for children.

Key Vocabulary



App-Level Control: Managing settings and usage limits for individual apps.

Privacy Settings: Options within an app to control who can see information or contact the child.

Notifications Management: Controlling alerts to reduce distractions.

In-App Purchases: Buying items or virtual currency within an app.

Screen Time / Usage Limits: Restricting how long a child can use a specific app.

Warm-Up / Discussion Prompt

- Ask: "Which apps do your children use the most? Games, social media, video platforms?"
- Scenario: A child spends 3 hours on a single game daily, ignoring homework. What can you do using app-specific controls?
- Invite parents to share challenges they face with **app addiction or privacy concerns**.

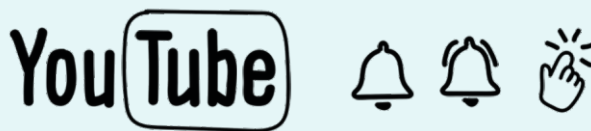
Core Activity - Hands-On / Simulation

Step 1 – Demonstration:

- Show screenshots or live demo of **popular app-level controls**:
 - o **YouTube:** Restricted Mode, content filters, screen time limits.
 - o **Instagram:** Privacy settings, comment filters, time reminders.
 - o **Gaming Apps:** In-app purchase restrictions, playtime limits.

YouTube – Step by Step (Mobile & Desktop)

Restricted Mode, content filters, and screen time limits



Step 1 – Settings

- Open YouTube → tap profile icon → **Settings**.

Step 2 – Restricted Mode

- Go to **General** → **Restricted Mode** → turn ON (filters mature content).

Step 3 – YouTube Kids (Better for Young Children)

- Install **YouTube Kids** → choose age group (Preschool/Younger/Older).

- Block channels/videos if needed & review watch history.

Step 4 – Screen Time Limits

- YouTube app → **Remind me to take a break** (set interval).
- YouTube Kids → **Profile** → **Timer** (set daily limit).
- For stricter limits, use **Family Link (Android)** or **Screen Time (iOS)**.

Step 5 – Privacy & Comments

- Set uploads to **Private/Unlisted**.
- Limit or disable comments.
- Turn off location sharing.

Step-by-step guide for Instagram controls

Privacy, Comment Filters, Time Reminders



Step 1 – Open Settings

- Instagram → Profile → Menu (☰) → **Settings**.

Step 2 – Privacy

- **Private Account** → only approved followers see posts.
- **Activity Status OFF** → hides online status.
- **Story Controls** → choose who can view/reply.
- **Blocked Accounts** → block unwanted contacts

Step 3 – Comments

- **Allow Comments From** → choose followers/friends.
- **Block Comments From** → add specific accounts.
- **Hide Offensive Comments ON**.
- **Manual Filter** → add bad words to block

Step 4 - Screen Time

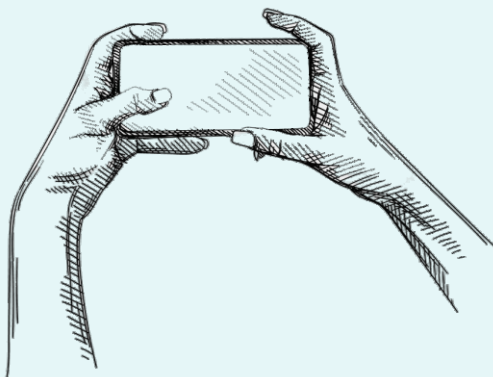
- **Your Activity** → **Set Daily Reminder** for usage limits.
- For stricter limits, use **iOS Screen Time** or **Google Family Link**.

Step 5 - Extra Safety

- **Restrict Accounts** → limit interactions quietly.

Report bullying, spam, or harmful content.

Gaming Apps - Step by Step (In-App Purchases & Playtime Limits)



Step 1 - Open Settings

- **iOS:** Settings → Screen Time → Content & Privacy → iTunes & App Store Purchases.
- **Android:** Play Store → Profile → Settings → Family → Parental Controls.

Step 2 - Restrict Purchases

- **iOS:** In-App Purchases → **Don't Allow**; require passcode for purchases.
- **Android:** Turn on Parental Controls → require authentication; set age ratings.

Step 3 - Set Playtime Limits

- **iOS:** Screen Time → App Limits → **Games** → set daily limit.
- **Android (Family Link):** Child's profile → Screen Time → set daily limit or bedtime lock.

Step 4 - Monitor Usage

- Review activity reports: games played, time spent, frequency.

Guided Discussion



- Why is it important to control apps individually rather than just overall device usage?
- How do privacy settings protect children from strangers or unwanted attention?
- How can time limits and notifications control help children develop healthy habits?

Discuss the balance between freedom and safety in app usage

Wrap-Up

- **See – Control – Discuss:** Monitor app usage, set appropriate limits, and talk with children about responsible use.

- App-level controls complement **OS-level parental controls**.

Regularly review **privacy and safety settings** as apps update frequently

Extension / Homework

Parents check their child's top 5 apps and apply one control in each (time limit, content filter, or privacy setting).

6.3 Network-level controls (DNS filters, router settings)

Learning Objectives

By the end of this session, parents will:

1. Explain in simple terms what network-level controls are and how they protect children online.
2. Identify tools like DNS filters and router settings that help block harmful content.
3. Take practical steps to set up basic safety measures at home on Wi-Fi networks.

Key Vocabulary



Network – The connection that links all devices in your home to the internet.

Router – The device that shares the internet with all your devices.

DNS Filter – A tool that blocks unsafe websites before they even open.

Firewall – A protective shield that stops unwanted content or visitors from reaching your network.

Parental Controls – Settings on devices or the router that limit access to certain websites or apps.

Router dashboard – the web page where you configure your home router.

DNS – like the phone book for the internet; changing it can enable category-based filtering.

MAC address – a device's unique hardware ID. Routers use it to identify and apply rules to devices.

Parental Controls / Access Control / Web Filter – menu names where blocking/time limits live.

Warm-Up / Discussion Prompt

- Ask parents: "Have you ever noticed your child stumbling across videos or websites you didn't want them to see?"
- Scenario: "Imagine your child tries to open a game or video that isn't appropriate, but it doesn't load. How would that feel? That's what a DNS filter does."

Core Activity



Router-based Parental Controls:

Step 1 – Find Router IP & Log In

- **Windows:** ipconfig → Default Gateway.
- **Mac:** Settings → Network → Wi-Fi → Advanced → Router.
- **iPhone/Android:** Wi-Fi → Network → (i)/Advanced → Router.
- Open browser → type IP (e.g., 192.168.1.1) → log in with admin details (see router sticker if unsure).
- **Tip:** Change the default admin password immediately.

Step 2 – Block Unsafe Websites

- Go to **Parental Controls / Security** → **URL Filter**.
- Add rule: **Block example.com** (or *.example.com for subdomains).
- Apply to child's device(s) → Save.
- Test by visiting the site.

Step 3 – Set Internet Time Limits

- Create a profile for your child's device.
- Set **allowed hours** (e.g., weekdays 7am–8:30pm, weekends 9am–9pm).
- Save & enable.

Windows DNS filter setup:

Step 1 – Open Network Settings

- Press **Win + R** → **ncpa.cpl** → Enter.
- Right-click active connection (Wi-Fi/Ethernet) → **Properties**.

Step 2 – Set IPv4 DNS

- Select **Internet Protocol Version 4 (TCP/IPv4)** → **Properties**.
- Choose **Use the following DNS server addresses**:
 - o **OpenDNS FamilyShield**: 208.67.222.123 / 208.67.220.123
 - o **Cloudflare Family**: 1.1.1.3 / 1.0.0.3
 - o (Google DNS: 8.8.8.8 / 8.8.4.4 – not filtered)
- Click **OK** → **Close**.

Step 3 – Set IPv6 DNS (Optional)

- Select **Internet Protocol Version 6 (TCP/IPv6)** → **Properties**.
- Enter:
 - o **OpenDNS FamilyShield**: 2620:119:35::123 / 2620:119:53::123
 - o **Cloudflare Family**: 2606:4700:4700::1113 / 2606:4700:4700::1003

Guided Discussion

- **Ask parents:**
 - o “How easy or difficult did you find setting up the DNS filter?”
 - o “What types of websites or apps would you want to block for your child?”
 - o “How can these tools help reduce stress about what children see online?”
- Connect activity to real life: Emphasize that while tools help, conversations about safe internet habits are still necessary.

Wrap-Up

"Safe network, safe child."

- **Key Takeaways:**
 1. DNS filters and router settings are like a digital gatekeeper.
 2. They protect children before harmful content even reaches their device.
 3. Network-level controls are most effective when combined with guidance and supervision.

Extension / Homework



- Parents check and list all devices connected to home Wi-Fi.
- Set up at least one DNS filter or basic parental control on the router.
- Discuss with children what content is allowed online and why.

6.4 Browser-based tools and safe search options

Learning Objectives

By the end of this session, parents will:

- Understand what browser safety tools and **SafeSearch** are, and why they matter.
- Enable SafeSearch and similar filters on common browsers (Google Chrome, Edge, Safari, Firefox).
- Teach children to use search responsibly and avoid unsafe or inappropriate content.
- Recognize that these tools help but are not **foolproof**; parental guidance is still essential.

Key Vocabulary

Browser – The app used to visit websites (e.g., Chrome, Safari).

SafeSearch – A search engine filter that blocks explicit or harmful results.

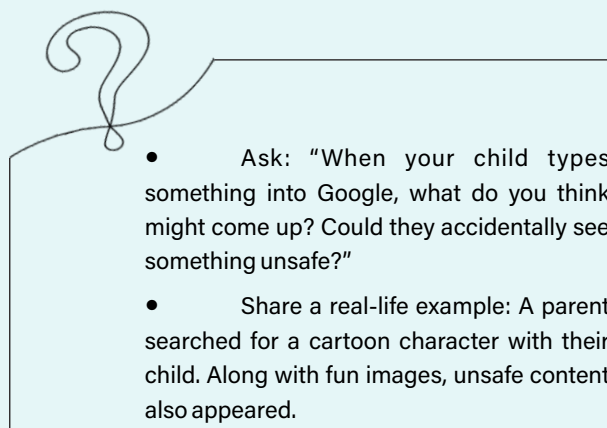
Extension / Add-on – Small tools parents can add to browsers to block ads, filter content, or limit distractions.

Pop-ups – Small windows or ads that suddenly appear when browsing.

Phishing – Fake websites or links designed to trick users into giving away information.

Safe Browsing – feature that blocks phishing, malware and some unsafe pages.

Warm-Up / Discussion Prompt



Core Activity

Enable Safe Search and Safe Browsing in Browsers

Google Chrome – Desktop (Windows / macOS)

SafeSearch (Filters Explicit Results)

- On **PC/Chrome**: google.com → Settings → **Search settings** → turn on SafeSearch → Save.
- On **Mobile**: Chrome app → google.com → Menu → **Search settings** → turn on SafeSearch → Save.

Safe Browsing (Protects from malware & phishing)

- Chrome → Menu (:) → **Settings** → **Privacy & security** → **Security**.
- Choose **Enhanced protection** (best) or **Standard protection**.
- On mobile: Chrome app → Settings → Privacy & security → Safe Browsing → choose protection level.

YouTube – Restricted Mode (works across browsers & app)**Web (desktop)**

1. Go to **youtube.com**.
2. Click your profile icon (top-right) → at the bottom of the menu toggle **Restricted Mode** to **On**.

Mobile app

1. Open the YouTube app → tap your profile → **Settings** → **General** → **Restricted Mode** → turn **On**.

Guided Discussion

- Why is SafeSearch important, but not enough by itself? (Kids can still click unsafe ads, or use other apps without filters.)
- What should parents do if children come across inappropriate results despite filters?
- How can browser tools be combined with parental conversations about curiosity, respect, and safe online searching?

Wrap-Up

Reinforce 3 key points:

Turn on SafeSearch on every browser/device children use.

Extension / Homework

Parents and children together enable SafeSearch on all home devices (phones, tablets, PCs).

Note



Emerging AI Threats



- 7.1** Deepfakes: recognising manipulated media
- 7.2** AI chatbots & grooming risks
- 7.3** Fake profiles and automated scam accounts
- 7.4** Teaching children media verification skills

Welcome to the cutting edge of digital safety. The internet is constantly evolving, and so are its risks. This chapter will prepare you for a new wave of threats powered by Artificial Intelligence (AI).

Think of it this way: a simple scammer might use a fake name, but an AI-powered scammer can create a realistic fake person with a convincing voice and a detailed backstory.

This chapter is designed to help you and your child become a new kind of digital detective, capable of recognizing threats that are often invisible to the naked eye.

Here's a roadmap of what we will cover:

- **Deepfakes: Recognising Manipulated Media:** Learn how to spot deepfakes—videos, images, or audio clips that have been altered by AI to show someone saying or doing something they never did. We'll give you clear, non-technical signs to look for so you can tell what's real from what's not.
- **AI Chatbots & Grooming Risks:** Understand how AI is used to create realistic chat experiences. We'll discuss the dangers of AI chatbots being used to groom children by building trust and manipulating conversations.
- **Fake Profiles and Automated Scam Accounts:** Discover how AI is used to create entire fake profiles and automated accounts that can quickly spread scams and misinformation.
- **Teaching Children Media Verification Skills:** This is the most important section. We'll provide you with practical, hands-on activities to teach your child how to question what they see online and use simple tools to verify media.

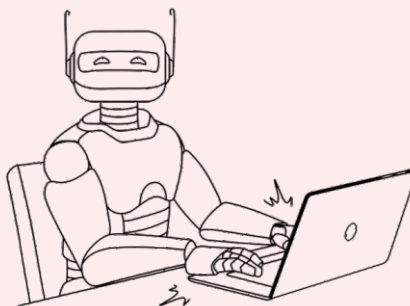
7.1 Deepfakes: Recognising Manipulated Media

Learning Objectives

By the end of this session, parents will:

- Understand what deepfakes are and why they are increasingly used online.
- Identify common signs of manipulated photos, videos, and audio.
- Discuss real-life risks of deepfakes with their children (misinformation, bullying, scams).
- Take practical steps to verify content and guide children on safe media consumption.

Key Vocabulary



Deepfake – A photo, video, or audio clip created using AI to make it look or sound real, even though it's fake.

Manipulated Media – Any media that has been digitally altered to mislead or trick viewers.

Misinformation – False or misleading information shared without harmful intent.

Verification – Checking if content is genuine using trusted sources

Warm-Up / Discussion Prompt

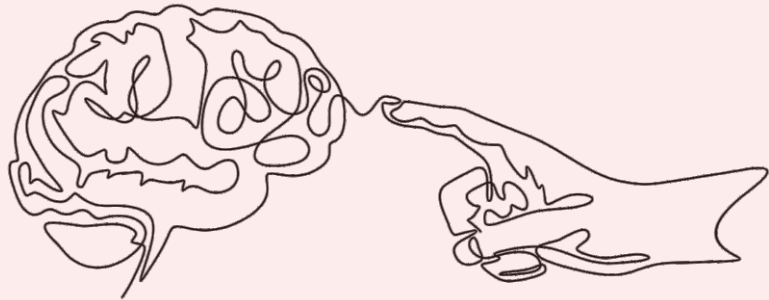
- Ask: "Have you ever seen a funny video where someone's face was swapped with a celebrity's?"
- Share a safe, light-hearted example (e.g., a famous actor's face swapped into a cartoon scene).
- Then ask: "What if the same technology was used to trick people or embarrass someone unfairly?"

Core Activity

Spot the Fake

1. Show parents pairs of short clips/images: one genuine, one manipulated (use harmless deepfake demo videos available online).
2. Ask them to look for small signs (lip-sync mismatches, odd lighting, blurry edges, unnatural voice).
3. Use an answer key to reveal the correct answers.

Guided Discussion



- Why do people make deepfakes? (fun, satire, scams, harassment).
- How can children be affected? (loss of trust, bullying, embarrassment, believing false info).
- How can parents respond?
 - o Teach kids to **pause before believing or sharing** content.
 - o Encourage them to **come to a parent/teacher** if unsure.
 - o Use tools like **Google Reverse Image Search** or trusted news sources for verification.

Wrap-Up- Mantra

"Not everything you see or hear online is real — pause, check, and then decide."

- Remember: If something feels “off,” it probably is.
- Teach children to look closely, ask questions, and confirm with reliable sources.

Extension / Homework

Pick one viral photo/video from social media and work with their child to verify its authenticity using fact-checking sites (**e.g., Snopes, Alt News, or Google Fact Check Tools**).

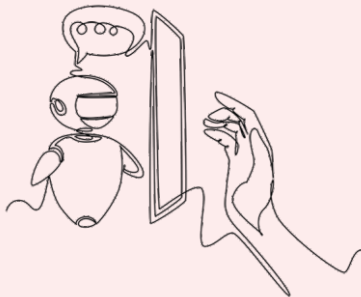
7.2 AI Chatbots & Grooming risks

Learning Objectives

By the end of this session, parents will:

- Understand what AI chatbots are and how children may interact with them online.
- Recognise how predators may misuse chatbots or online chats for grooming.
- Learn practical ways to guide children to use chatbots safely.
- Know what red flags to watch for in conversations their children may be having online.

Key Vocabulary



AI Chatbot – A computer program that uses artificial intelligence to “chat” like a human.

Grooming – When someone builds trust with a child online to exploit or harm them.

Trust-Building – Friendly conversations used by predators to lower a child's guard.

Red Flags – Warning signs that something may be unsafe (e.g., asking for secrets, moving conversations to private apps).

Warm-Up / Discussion Prompt

- Ask parents: "Have your children ever used Siri, Alexa, or a chatbot that answers questions or talks back?"
- Share a relatable scenario: A child plays with an AI chatbot for homework help but ends up spending hours chatting casually with it.

Core Activity

Spot the Red Flags

1. Provide parents with **sample chat transcripts** (one safe chatbot helping with math, one suspicious "chatbot" asking for personal details).
2. Ask them to highlight phrases that are concerning (e.g., "Don't tell your parents," "Can we chat on another app?").

Guided Discussion



- What are the benefits of chatbots? (homework help, learning, entertainment).
- What are the risks? (children oversharing, grooming attempts, addictive chatting).
- How can parents protect children?
 - o Teach children never to share personal info with any chatbot or online chat.
 - o Remind them that not all chatbots are real AI — sometimes it could be a person pretending.
 - o Encourage open conversations: "If a chatbot says something odd or makes you uncomfortable, come tell me."
 - o Use parental controls to limit which apps/websites children can access.

Wrap-Up

- Children should enjoy technology but also learn healthy limits.
- Parents should supervise new apps and stay curious about what their child is using.

Extension / Homework

Parents and children together: Explore a safe chatbot (like an educational assistant) and discuss how it differs from risky platforms.

7.3 Fake profiles and automated scam accounts

Learning Objectives

By the end of this session, parents will:



- Understand what fake profiles and automated scam accounts are.
- Recognise the warning signs of suspicious accounts online.
- Learn how scammers use fake identities to deceive children.
- Practice simple steps to guide children in spotting and avoiding these risks.

Key Vocabulary

Fake Profile – A social media or online account made with false details (fake name, fake photo).

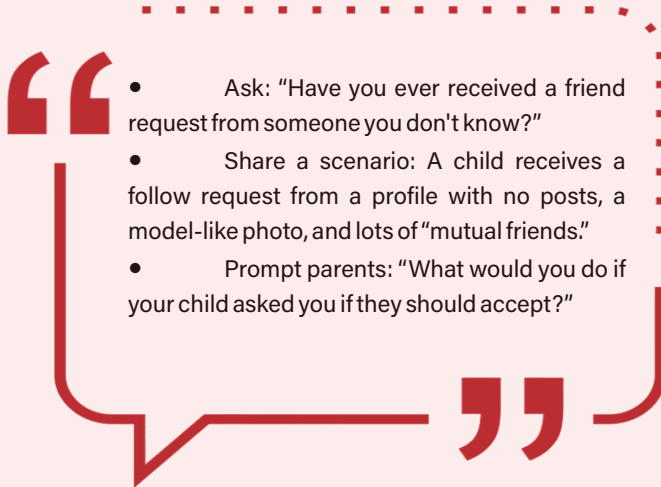
Bot Account – An automated account controlled by software, not a real person.

Catfishing – Pretending to be someone else online to trick others.

Scam – A dishonest scheme to steal money, information, or trust.

Red Flags – Warning signs that an account may be fake (few friends, generic photos, strange messages)

Warm-Up / Discussion Prompt



- Ask: "Have you ever received a friend request from someone you don't know?"
- Share a scenario: A child receives a follow request from a profile with no posts, a model-like photo, and lots of "mutual friends."
- Prompt parents: "What would you do if your child asked you if they should accept?"

Core Activity

Spot the Fake Profile

1. Show parents 2–3 sample social media profiles (one real, one fake, one automated bot-like).
2. Ask them to identify red flags (stock image profile picture, very few posts, strange links, lots of followers but no real engagement).
3. Debrief: Why would a scammer or bot make such a profile?

Guided Discussion

- Why are children more vulnerable to fake accounts? (curiosity, wanting more friends, not recognising scams).
- How do bots trick users? (likes, follows, fake giveaways, links to phishing sites).
- Key strategies for parents:
 - o Teach children not to accept friend requests from strangers.
 - o Encourage them to check profiles carefully before engaging.
 - o Use privacy settings to limit who can send requests/messages.

Wrap-Up

"Not every profile is a person.
Think twice before you

- Children should know: If it feels suspicious, it probably is.
- Parents should remind children: It's safer to have fewer, real friends than many fake ones.

Extension / Homework

Parents and children together:

Review the child's current friend/follower list and remove any unknown or suspicious accounts.

7.4 Teaching children media verification skills

Learning Objectives

By the end of this session, parents will:



- Understand why children need skills to check whether online content is real or fake.
- Learn simple, child-friendly techniques to verify information, images, and videos.
- Guide children in questioning what they see, read, and share online.
- Build habits of critical thinking and responsible sharing.

Key Vocabulary

Misinformation – False or misleading information spread by mistake.

Disinformation – False information spread on purpose to trick people.

Source – The origin of information (who posted or created it).

Verification – The process of checking if something is true.

Fact-checking – Using trusted websites or tools to confirm if news is correct.

Warm-Up / Discussion Prompt

- Ask: "Have you ever shared a funny picture or news online that later turned out to be fake?"
- Share a scenario: A child sees a WhatsApp forward saying, "A celebrity has given away free phones!"
- Ask parents: "What do you think your child might do if they saw this? Would they believe it?"

Core Activity



Spot the Fake News Headline

1. Show parents 2–3 headlines (one real, one fake, one exaggerated).
2. Ask: How can you tell if it's trustworthy? (check the source, too dramatic wording, no supporting evidence).
3. Discuss strategies children can learn: "Pause, Question, Verify."

Image Check (Reverse Image Search Demo)

- Demonstrate using **Google Reverse Image Search** or **TinEye** with a suspicious viral photo.
- Show how the same photo might appear in different contexts or years.

Encourage parents to try this at home with children

Wrap-Up

"Pause. Check.
Share only if true."

- Teach children to stop before believing or forwarding anything online.
- Remind them: Not everything on the internet is what it looks like.

Extension / Homework



Take one piece of viral content they've seen recently (a WhatsApp forward, Instagram post, or YouTube video) and verify it together.

Note

Note

Communication & Trust Building



- 8.1 “Talk + Tech” strategy: balancing rules with open conversation**
- 8.2 Avoiding over-control to maintain trust**
- 8.3 Encouraging children to report problems without fear of punishment**
- 8.4 Role-play scenarios for difficult online situations**

This chapter is about building the strongest defense system of all: a strong, trusting relationship with your child.

Think of it this way: technology is like a car, and your child is the driver. You can install all the best safety features—airbags, seatbelts, and a GPS tracker—but none of them will work if your child is too scared to tell you they've had an accident. This chapter will help you become a proactive co-driver, not just a backseat monitor.

Here's a roadmap of what we will cover:

- **"Talk + Tech" Strategy:** Balancing Rules with Open Conversation: Learn why a combination of clear rules and continuous, honest dialogue is far more effective than either one alone.
- **Avoiding Over-Control to Maintain Trust:** Understand the dangers of helicopter parenting in the digital world. We'll show you why giving your child a degree of freedom and trust can actually lead to better decision-making.
- **Encouraging Children to Report Problems Without Fear of Punishment:** Discover how to create a safe space where your child feels comfortable telling you about mistakes or scary situations without worrying they'll lose their privileges.
- **Role-Play Scenarios for Difficult Online Situations:** Get hands-on with practical exercises that prepare both you and your child for real-life challenges, from a mean comment to a scary message.

8.1“Talk + Tech” strategy: Balancing rules with open conversation

Learning Objectives

By the end of this session, parents will:

- Understand why technology rules alone are not enough to keep children safe online.
- Learn the importance of combining technical tools (filters, parental controls) with ongoing, open conversations.
- Develop strategies to build trust so children feel safe coming to parents when something goes wrong online.
- Create a balanced home environment where technology supports safety and healthy habits.

Key Vocabulary

Parental Controls – Settings that limit or monitor what children can access online.

Digital Boundaries – Family-agreed rules about device use (time, apps, websites).

Trust Circle – An environment where children feel safe to share concerns without fear.

Open Conversation – Talking regularly and honestly about online life without judgment.

Tech + Talk Balance – Using both technology tools and ongoing conversations to protect children.

Warm-Up / Discussion Prompt

- Scenario: “Imagine your child comes across a scary video online. Would they feel comfortable telling you—or would they hide it, afraid of getting into trouble?”
- Ask parents: “How do you think your child would respond? Why?”
- Reflection: Highlight that controls can block some risks, but children will still face things—conversation builds resilience.

Core Activity



Build a “Family Digital Agreement”

- Parents draft a sample family tech agreement with two parts:
 1. **Tech Rules** – e.g., screen time limits, SafeSearch on, no devices at dinner.
 2. **Talk Promises** – e.g., “I will listen without shouting,” “I won’t punish you for telling me about mistakes,” “We’ll review rules together every month.”

Guided Discussion

- Why do children sometimes hide online problems from parents? (fear of punishment, loss of device, being misunderstood).
- How can parents balance guidance with listening?
- What are the risks of only relying on tech tools without conversation? (kids bypass rules, secrecy, lack of resilience).
- What happens if there’s talk without tech? (rules missing, exposure to harm).

Wrap-Up

Tech sets the limits,
Talk builds the trust.”

Rules protect children, but trust helps them navigate the unexpected

Extension / Homework

Choose one new tech rule (e.g., no devices in bedrooms).

Encourage children to share one thing they enjoyed online and one thing that bothered them.

8.2 Avoiding over-control to maintain trust

Learning Objectives

By the end of this session, parents will:

- Recognize the difference between healthy supervision and over-control in children's digital lives.
- Understand how excessive restrictions can damage trust and push children toward secrecy or risky behaviour.
- Learn strategies to set limits while still respecting children's growing independence.
- Build a balanced approach where safety, trust, and open communication go hand-in-hand.

Key Vocabulary



Over-Control – Excessive monitoring or restrictions that make children feel mistrusted.

Digital Autonomy – A child's ability to make age-appropriate decisions about online activities.

Trust Balance – The balance between protecting children and respecting their independence.

Secrecy Spiral – When children hide online activities because they fear punishment or judgment.

Guided Freedom – Allowing children controlled independence with clear boundaries and conversations.

Warm-Up

Ask parents: "When you were a child, what was one rule that felt 'too strict' at home? How did you respond—did you obey, sneak around it, or rebel?"

Core Activity

"Trust Contract" Design

- Parents, in small groups, design a short "Trust Contract" with their imaginary child:
 - What parents will do (set filters, time limits, check devices occasionally).
 - What children agree to do (share concerns, follow limits, ask before downloading apps).

Guided Discussion

- Why do children sometimes hide things online?
- How does over-control affect a child's confidence and honesty?

Wrap-Up

**"Control protects.
Trust connects."**

- Too much control = secrecy and distance.
- Too little control = exposure to risks.
- Balanced control + open trust = safer, stronger digital habits.

Extension / Homework

- Parents create a **"3-2-1 Plan"** at home:
 - o 3 rules they'll keep for safety (filters, screen-free zones, limits).
 - o 2 freedoms they will allow their child (choosing games, limited private chats).
 - o 1 promise to build trust (e.g., "I won't check your phone without asking first").

8.3 Encouraging children to report problems without fear of punishment

Learning Objectives

By the end of this session, parents will:

- Understand why children often hide online problems instead of reporting them.
- Recognize how fear of punishment or blame prevents children from seeking help.
- Practice responses that encourage openness and trust when children disclose online challenges.

Key Vocabulary

Safe Space – An environment where children feel comfortable sharing without fear of punishment.

Blame-Free Listening – Listening without immediately criticizing or scolding.

Open Door Policy – Letting children know they can approach parents anytime with problems.

Supportive Response – A calm, reassuring reaction that focuses on solutions, not blame.

Early Reporting – When children share concerns quickly before a situation worsens.

Warm-Up / Discussion Prompt

- Ask parents: "When you were young, did you ever hide a mistake or problem from your parents? Why?"
- Transition: Children today do the same—especially with online mistakes—because they fear punishment more than the problem itself.



Core Activity

"What's the Message?"

- Show 3 sample parent responses:
 1. "Why did you do that? You should know better!"
 2. "Thank you for telling me. Let's fix this together."
 3. "If you make that mistake again, your phone is gone."
- Discuss: Which of these responses builds safety and which builds fear?

Guided Discussion



- Why do children fear punishment more than online risks?
- What long-term effects can harsh reactions have on honesty and trust?
- How can parents strike a balance between correcting mistakes and encouraging reporting?

Wrap-Up

"Listen First. Guide Second."

- A calm reaction today ensures your child will come to you tomorrow.
- Children need help, not fear, when problems arise online.

Extension / Homework

If your child makes a mistake (big or small), respond first with understanding, then with guidance.

8.4 Role-play scenarios for difficult online situations

Learning Objectives

By the end of this session, parents will:



- Recognize common challenging situations children face online (cyberbullying, peer pressure, stranger danger, oversharing).
- Practice supportive, non-punitive ways to guide children through these situations.
- Develop confidence in using role-play at home as a tool for teaching digital safety.
- Build strategies that encourage children to think before acting and seek help when needed.

Key Vocabulary

Cyberbullying – Using digital platforms to harass, threaten, or embarrass someone.

Peer Pressure – Influence from friends or classmates to behave in a certain way, online or offline.

Stranger Contact – Unfamiliar people initiating communication online.

Oversharing – Sharing too much personal information on social media or chats.

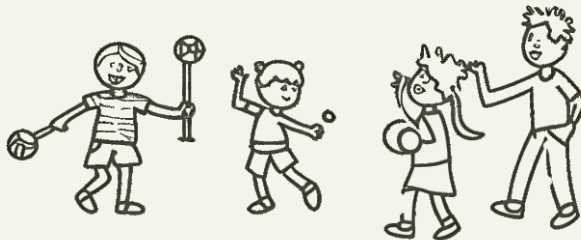
Role-Play – Acting out a situation to practice real-life responses.

Warm-Up / Discussion Prompt

- Ask parents: “Imagine your child comes to you and says, ‘Someone was mean to me online’—what’s the first thing you would say?”
- Share a real-life example: A 12-year-old girl stopped using her favorite game because strangers kept messaging her, but she never told her parents because she feared losing screen time.

Core Activity

Role-Play




Divide parents into small groups.

1. Assign each group a scenario to act out:
 - o **Scenario A:** Your child shows you a mean message sent by a classmate.
 - o **Scenario B:** Your child says a new “friend” online is asking for personal photos.
 - o **Scenario C:** Your child admits they posted something embarrassing about themselves and now regret it.
 - o **Scenario D:** Your child wants to join a trending challenge that looks unsafe.
2. Each group acts out both roles: parent and child.
3. After the role-play, groups share what responses worked best to keep communication open.

Guided Discussion

- Which role-play scenarios felt realistic?
- How did different reactions change the child's willingness to share?
- What's the balance between correcting mistakes and maintaining trust?
- How can role-play at home prepare children to make safer choices online?

Wrap-Up



"Practice the problem
before it happens."

- Just like fire drills prepare children for emergencies, role-play prepares families for online challenges.
- When children have practiced safe responses, they feel less afraid and more confident in real-life situations.

Extension / Homework

- Parents choose one scenario from the Role-Play Deck and practice it with their child.
- "If your child tells about a problem, you should listen calmly."

Note

Cyber Division
Cyber Headquarters, PHQ
Thiruvananthapuram