

Online Safety Guide for Parents

HOW TO PROTECT YOUR KIDS IN A CONNECTED WORLD

HAGAR

Every day, our kids and teens learn, explore and connect online.

But the internet can have a dark side, and not everyone who uses it has the right intentions.



After 30 years of working with survivors of human trafficking and abuse, Hagar is acutely aware of how vulnerable children and teens are to being exploited online, regardless of where in the world they live.

That's why we've created this guide.

To help you help your kids stay safe online.

Inside:

03 Your Guide to Keeping Your Kids & Teens Safe Online

04 Know the Current Landscape

05 5 Tips for Online Safety

06 Know The Signs of Online Abuse

07 Platform Checklists

08 Global Problem, Local Action



Your Guide to Keeping Your Kids & Teens Safe Online

Stay curious, calm, and connected

The most powerful safeguard for kids and teens is connection. When you create a safe space for open conversations about tech, you forge a firm foundation for online safety. Normalise sharing about online experiences (including mistakes), and affirm that you'll always support them even if something goes wrong.

Use a Family Tech Agreement

A family tech agreement is a set of expectations that you agree to as a family to manage screen usage. A family tech agreement can include device rules, which apps are okay and which aren't (and why), and where, when, and for how long devices can be used.

Teach Digital Citizenship

Kids and teens have new cultures and experiences at their fingertips - how cool! But there can be a dark side. Anything posted online can be copied, edited, and reposted. It can also last forever (**really**) on the internet. Discuss with your kids how our online behaviour can have lasting consequences not only for their reputations and online safety, but for others too.

Know the Current Landscape

Online exploitation is real, and it's growing. In fact, UNICEF estimates 1 in 10 children around the world have been victims of online exploitation. Online exploitation can include grooming, sextortion, non-consensual image sharing, and the creation and distribution of child sexual abuse material.

Grooming:

Grooming is a term used to describe the gradual but calculated process that an abuser uses to build trust and create an emotional connection with a child in order to gain access to that child and make them vulnerable to abuse or exploitation.

Sextortion

Sextortion is when a person uses a sexual image or video to blackmail or threaten a child for money or more content.

Sexting:

Sexting includes instant messages, texts, live chats or live webcam sessions that share images or video of a sexually explicit nature.



Child Sexual Abuse Material

Child Sexual Abuse Material (CSAM): Includes real images and those created with AI of sexual acts that involve a minor. CSAM includes webcam and live-streamed abuse, and any content that exploits or sexualises a child. Creating, sharing and possessing CSAM is a crime.

5 Tips To Keep Children & Teens Safe Online



1.
Set up family settings on every platform or operating system your devices use.
See safety checklists on page 7.



2.
Ensure **contact requests** are only enabled from people your child or teen knows in real life.



3.
Ensure your child or teen's **social media profiles** are set to **private.**



4.
Encourage your child or teen to **think before they post.** Would they want their friends, family or community to see what they share? *Remember, the internet is forever.*



5.
Remind your child or teen to **trust their instincts.** If something feels off or weird, it probably is - and they should tell someone they trust right away.



Know The Signs

Signs to Watch For

- Someone your child or teen doesn't know asks for photos.
- An online "friend" asks your child or teen to keep messages secret, or to move to a different app or program.
- Something about a chat or DM makes your child or teen feel pressured, confused, or uncomfortable.
- **If something feels 'off' it probably is.**

What to do if something goes wrong:

- Reassure your child they are not in trouble.
- Save all evidence including screenshots, usernames, payment info, etc.
- Block and report the user on the platform where it happened.
- Report to national hotlines or law enforcement (see below).
- Use **TakeItDown.ncmec.org** or **StopNCII.org** to remove explicit images.

Where to get help in New Zealand



- Immediate danger: Call **111.**
- New Zealand Police, non-emergency: Call **105** or make an **online 105 report.**
- Netsafe: Call **0508 NETSAFE (0508 638 723)** or text **4282** for free and confidential online-safety support.
- Department of Internal Affairs: Report online child sexual exploitation material through the Department's Digital Safety reporting service.
- Youthline: Free call **0800 376 633** or free text **234**, available 24 hours a day.

Platform Safety Checklists

Family Link (Google/Android/Chromebooks)



Set up screen time, app approvals, web filters, location sharing permissions, and School Time/Downtime. Use the official setup flow, not just Play Store settings.

- [ ] **Set up Family Link**
- [ ] **Enable SafeSearch**
- [ ] **Approve app installs**
- [ ] **Block Adult Sites**

Family Sharing (Apple iPhone/iPad/Mac)



Use your Apple device's Family Settings to manage child accounts with parental controls. You can set a passcode for screen time, manage content/privacy restrictions by age, and ensure communication & Siri/AI limits.

- [ ] **Set up Family Screen time settings with a passcode**
- [ ] **Enable downtime & communication limits**
- [ ] **Restrict explicit content**
- [ ] **Block unknown AirDrops & Contacts**

Family Safety (Microsoft Windows/Xbox)



Use Microsoft Family Safety to set up for content filters, screen time permissions, and app/site blocking. Make sure each child has their own account as part of the family so controls reflect their age.

- [ ] **Set up Family Safety on child/teen devices**
- [ ] **Limit screen time**
- [ ] **Filter web content**
- [ ] **Review friend lists**

Social Media



Most social media platforms offer built-in safety tools, including private accounts, content filters, messaging limits, and parental supervision features to create safer online experiences.

- [ ] **Set accounts to private**
- [ ] **Turn off location sharing**
- [ ] **Review followers regularly**
- [ ] **Report/block inappropriate users**



Global Problem, Local Action

What's happening in Southeast Asia?

Across Southeast Asia, children and teens just like our own are lured, threatened and exploited online. Sometimes, it's being forced to perform terrible acts on camera for paying viewers online. Other times it's being coerced into sharing harmful images and videos over messaging apps, which are then bought and sold on social media sites. Far too often, it's people from wealthy countries like New Zealand, who stream and pay for this content online.

No matter how it shows up, it's a crime against a child.

But there is good news.

Hagar teams work alongside police and other authorities to support investigations, while helping survivors heal and rebuild their lives, and training communities to stop exploitation before it starts.

Learn more about Hagar's work to prevent exploitation, support survivors, and bring traffickers to justice.