



Online Safety



Click the indicated image to view more details.

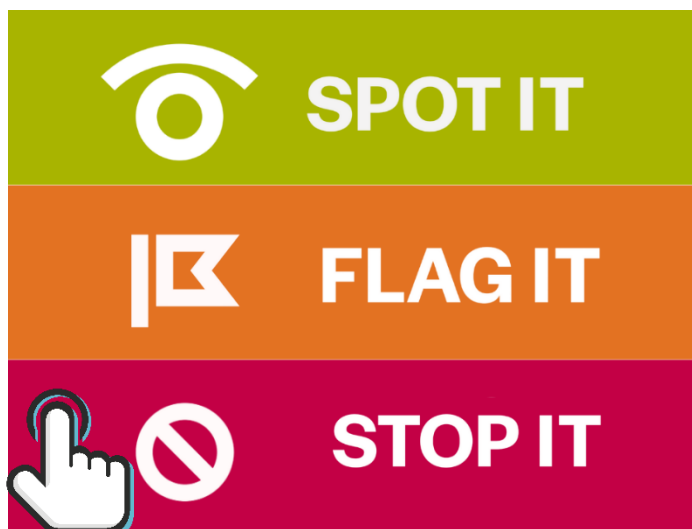


Coimisiún na Meán

Coimisiún na Meán enforces the binding [Online Safety Code](#) under the Online Safety and Media Regulation Act. It transitions digital safety from voluntary corporate policy to mandatory compliance.



Platform Obligations: Video-sharing and social media services are legally required to verify user age, suppress cyberbullying, and eliminate access to explicit or illegal content.



The "[Spot it, Flag it, Stop it](#)"

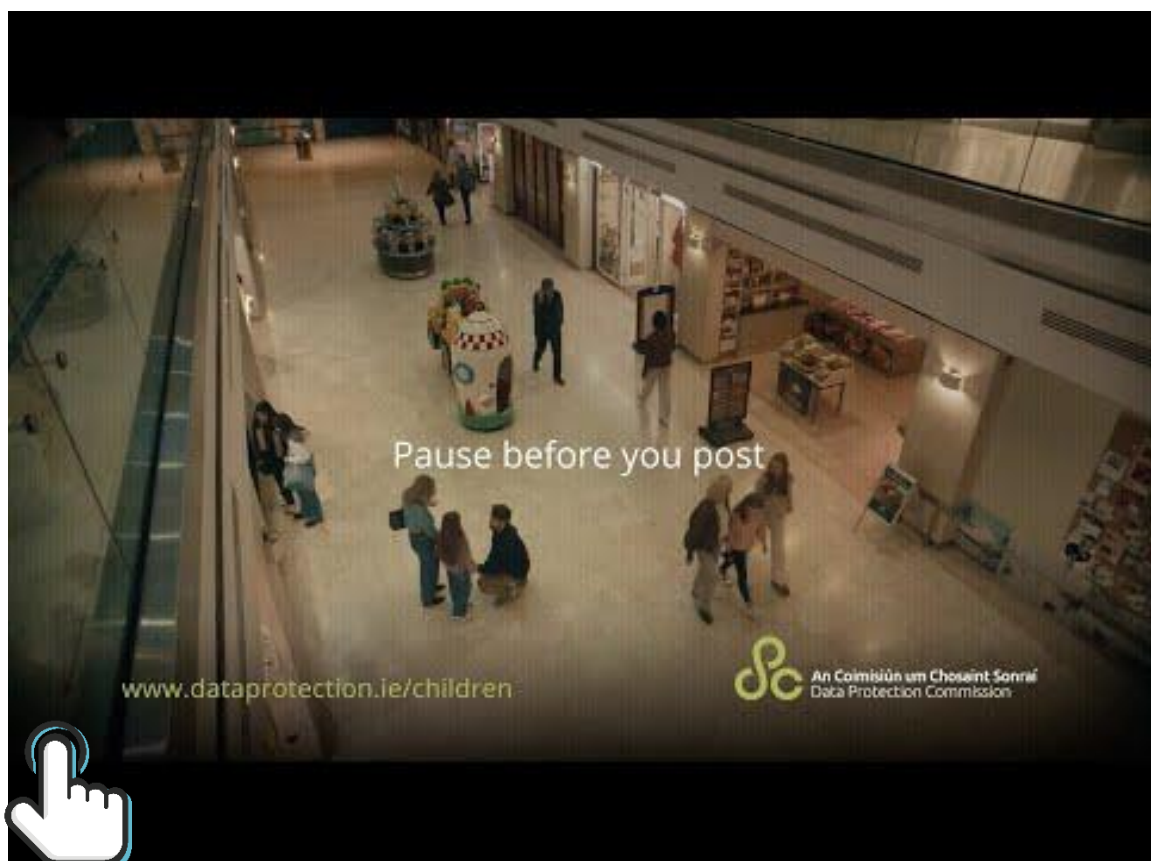
Protocol: The official regulatory reporting path. Harmful or illegal material must be reported directly to the platform hosting it first. If the platform fails to act, cases are escalated to the regulator to audit platform compliance.



The DPC enforces child-centric data privacy rules under the General Data Protection Regulation (GDPR).

The Fundamentals: This [statutory framework](#) dictates that commercial platforms must treat a child's data with heightened protection, restricting profiling, target-marketing, and intrusive data tracking.

The "Pause Before You Post" Initiative: A joint campaign with France's CNIL designed to educate parents on the long-term systemic dangers of digital oversharing.





An Roinn Dlí agus Cirt Department of Justice

Coco's Law: The Harassment, Harmful Communications and Related Offences Act establishes the non-consensual distribution of intimate images as a serious criminal offence. This law applies to both adults and minors, carrying severe criminal penalties

webwise.ie

WHAT IS COCO'S LAW?

Understanding the Harassment, Harmful Communication and Related Offences Act 2020 and the legal consequences of it for young people.

Ministry of Education

Co-financed by the Connecting Europe Facility of the European Union

No Excuses' Intimate Images Awareness Campaign

Public Awareness campaign from the Department of Justice Ireland highlighting the issue of sharing intimate images without consent. This short advert, part of the 'No Excuses' campaign, seeks to inform audiences of the recent changes in legislation in Ireland which criminalises the sharing of intimate images without consent



Information for Parents & Caregivers

Sharenting—the habitual posting of a child's life online—exposes minors to severe privacy violations before they are old enough to consent.



Sharenting

Pause Before You Post!



Misuse for Harmful Purposes

When we share online, we risk images being used in malicious ways. A recent study^[1] showed that only 20 images of a child are needed to create a deepfake video of them and parents upload an average of 63 images to social media every month!

Sharenting Risks

Digital Footprint

By sharing about their children online, parents are creating a digital footprint for their child from a very early age, that may be difficult to erase later on.





Unwanted Contact

Photos and videos contain information about the location and time at which they were taken (metadata, GPS data) which can reveal valuable information about your children.

Identity Theft and Fraud

Information revealed about a child such as their name, date of birth, school, etc. can be misused to hack passwords or for identity fraud scams.^[2]



Sharenting Tips

Limit your Audience

Set profile to "Private" and only share posts with close friends.

Avoid Oversharing

Cover your child's face or position them faced away from the camera and blur out any other identifiable information.



Location, Location

Turn off geo-location settings and ensure there is no other information within the image that could pinpoint your location.

Review your Posts

Regularly review the posts you have shared and delete any that you, or your child, are no longer comfortable sharing.

Have open discussions with your child before posting information about them on social media. Remember, it's their personal data you are sharing, not yours.



¹ *Expert warns parents over AI deepfakes of children* (RTÉ, May 2025)
² *'Sharenting' puts young at risk of online fraud* (BBC, May 2018)



An Coimisiún um Chosaint Sonraí
Data Protection Commission

AI Deepfake Training:

Research by Perspectus Global proves that only 20 public images of a child are required to train a generative AI model to build a realistic deepfake video.



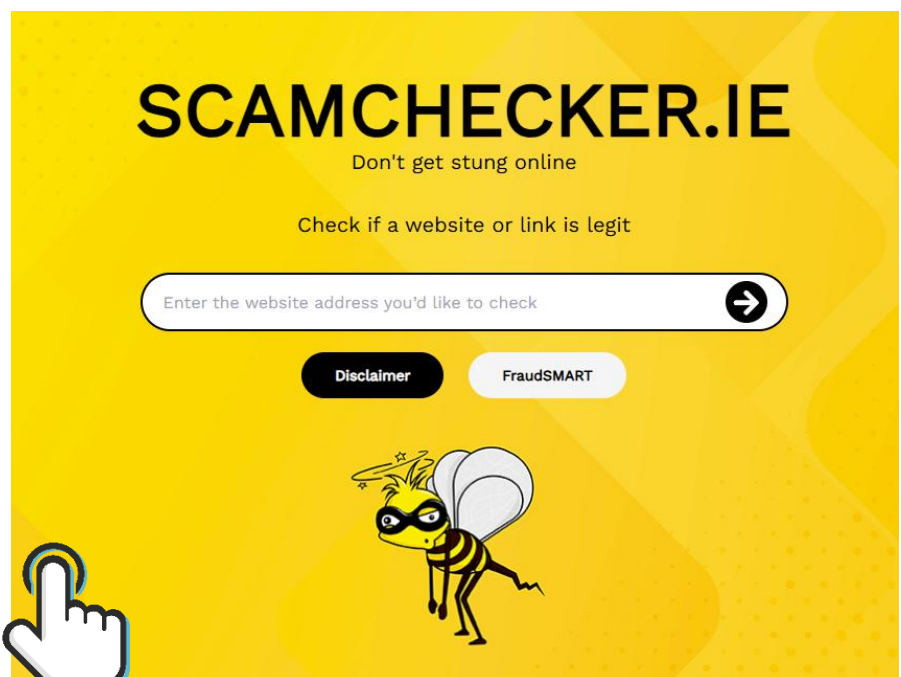
Metadata Leakage:

Digital photos embed hidden EXIF and GPS coordinates. Ill-intended individuals harvest this data to plot a child's training schedule, school location, and daily routines. [Electronic Frontier Foundation \(EFF\)](#)



Financial Identity

Theft: Sharing complete names, exact birth dates, and familial relations gives identity thieves the specific data points needed to bypass bank security systems or commit long-term financial fraud.



Paedo-Criminal Aggregation:

Official reports from the *Fondation pour l'enfance* show that **50% of**



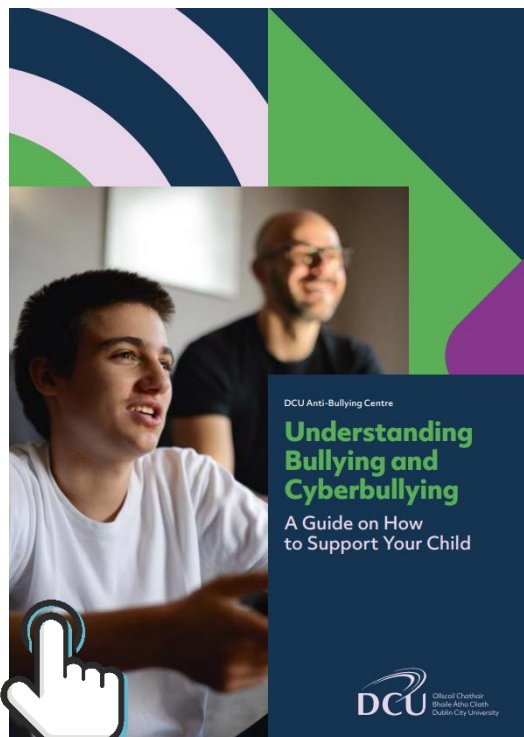
the children's photos discovered on paedo-criminal message boards

were originally published on public feeds by well-meaning parents.



Peer-to-Peer & Technical Threats

Cyberbullying & Burnout: Digital harassment has distinct characteristics due to its 24/7 nature. Curating highly manicured social feeds can lead to social media burnout, leaving children feeling isolated, jealous, or inferior.



Financial

Exploitation: Free-to-play online video games are designed with psychological loops that encourage kids to spend money via loot boxes, digital currency, and in-game passes.



You can help us reach more people with this campaign and increase pressure on decision-makers to make tech safe for kids

Download our toolkit which includes everything you need to get started!



Ireland-Childhood-Redrawn.zip

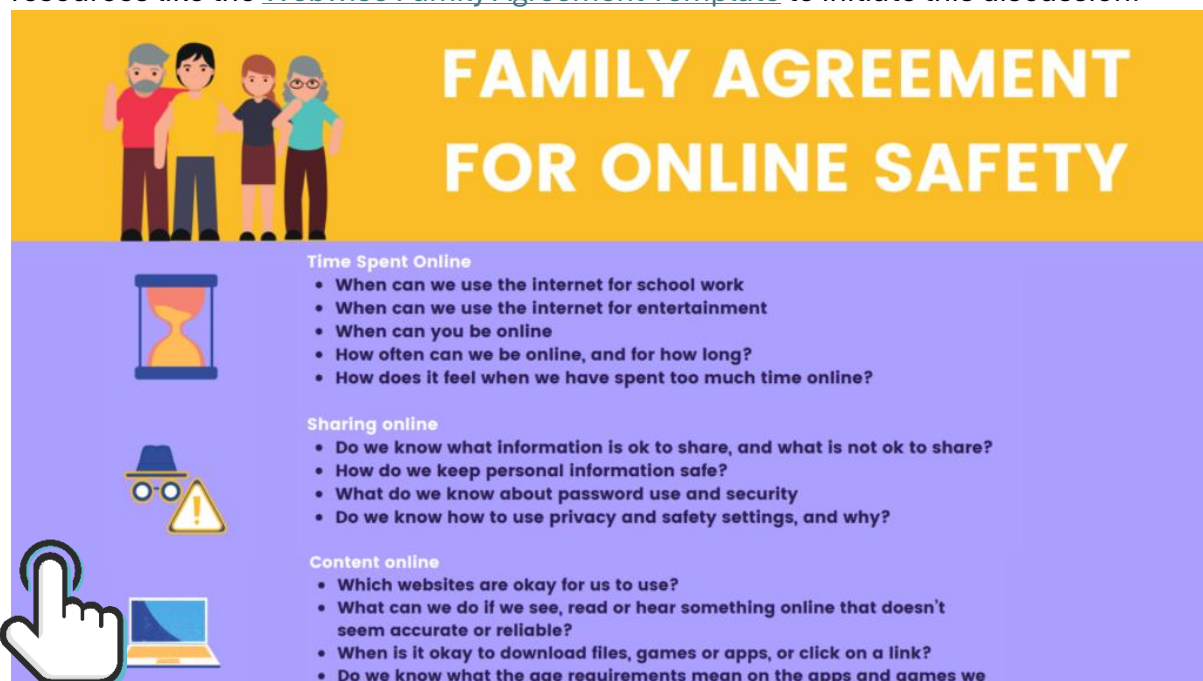


AI Friendship Disillusionment: Children frequently mistake conversational AI platforms and chatbots for actual companions. This dynamic, clouds their understanding of data privacy, as they willingly share deep personal secrets with a commercial algorithm.



Open Communication & Agreements

Establish a Family Agreement: Create a shared contract detailing acceptable screen time limits, approved applications, and proper online behaviour. Use resources like the [Webwise Family Agreement Template](#) to initiate this discussion.

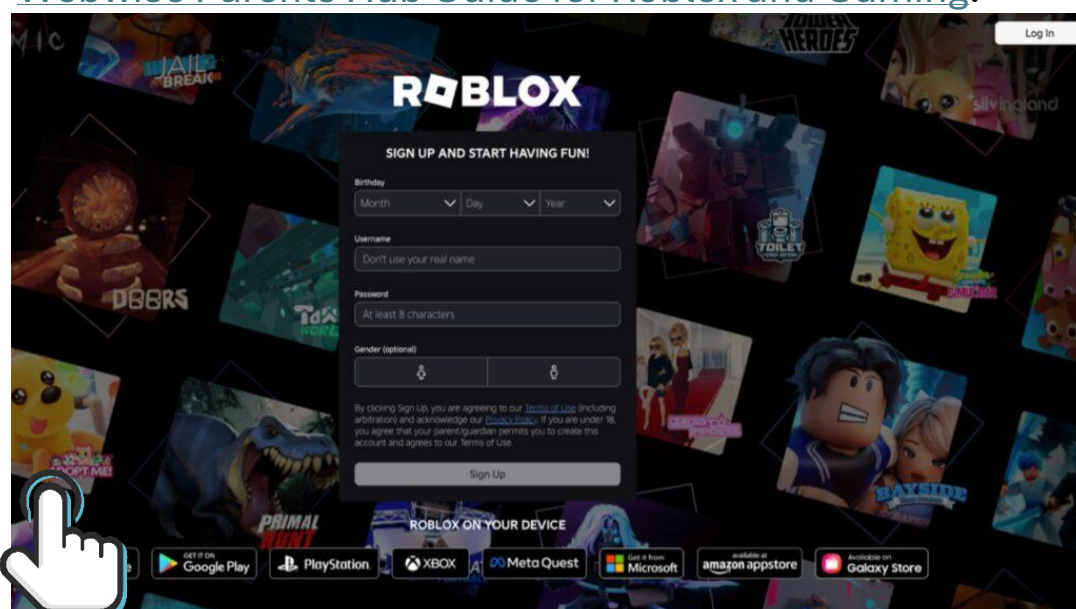


The poster is titled "FAMILY AGREEMENT FOR ONLINE SAFETY" in large white letters on a yellow background. Below the title, there are three sections on a purple background, each with an icon and a list of questions:

- Time Spent Online** (Icon: Hourglass):
 - When can we use the internet for school work
 - When can we use the internet for entertainment
 - When can you be online
 - How often can we be online, and for how long?
 - How does it feel when we have spent too much time online?
- Sharing online** (Icon: Magnifying glass over a warning sign):
 - Do we know what information is ok to share, and what is not ok to share?
 - How do we keep personal information safe?
 - What do we know about password use and security
 - Do we know how to use privacy and safety settings, and why?
- Content online** (Icon: Hand pointing at a laptop):
 - Which websites are okay for us to use?
 - What can we do if we see, read or hear something online that doesn't seem accurate or reliable?
 - When is it okay to download files, games or apps, or click on a link?
 - Do we know what the age requirements mean on the apps and games we

Co-Explore the Internet: Dedicate time to discover websites and play online games together. This establishes a positive baseline for tech use and makes children more likely to approach you if they encounter something troubling.

[Webwise Parents Hub Guide for Roblox and Gaming.](#)



The image shows the Roblox sign-up screen. The background is a collage of various Roblox game thumbnails. In the center, there is a "SIGN UP AND START HAVING FUN!" form with the following fields:

- Birthday: Month, Day, Year dropdowns
- Username: Text input with a hint "Don't use your real name"
- Password: Text input with a hint "At least 8 characters"
- Gender (optional): Male and Female radio buttons

Below the form, there is a "Sign Up" button and a small disclaimer: "By clicking Sign Up, you are agreeing to our [Terms of Use](#) (including arbitrators) and acknowledge our [Privacy Policy](#). If you are under 18, you agree that your parent/guardian permits you to create this account and agrees to our [Terms of Use](#)."

At the bottom, there is a "ROBLOX ON YOUR DEVICE" section with logos for Google Play, PlayStation, XBOX, Meta Quest, Microsoft, Amazon Appstore, and Galaxy Store.

Normalise "Oops" Moments: Assure your children that they can tell you if they make a mistake online or see something inappropriate, without the fear of immediate punishment or losing their devices.

[#TalkListenLearn Campaign](#)



**TALK
LISTEN
LEARN**



**Online Safety Talking
Points for Parents**
Developed by Irish Teens



An Roinn Oideachais
Department of Education



Co-financed by the Connecting Europe
Facility of the European Union

Technical Safeguards

Centralise Device Use: Keep computers and gaming systems in busy, communal areas of the home rather than private bedrooms.



Activate Parental Controls: Utilise built-in operating system tools (like Apple Screen Time or Google Family Link) to restrict adult content, manage screen limits, and block app downloads.



Disable In-App Purchases: Turn off purchasing capabilities or require password authentication for every transaction within device settings to prevent accidental financial charges.



Research Platforms: Check age ratings and privacy settings for popular platforms before allowing downloads. Resources like the [NSPCC A-Z App Guide](#) explain risks associated with individual social media channels.



Spotting Warning Signs

Monitor changes in your child's behaviour that might indicate cyberbullying, grooming, or exposure to disturbing content:

- Sudden sadness, anger, or frustration during or immediately after using a device.
- Becoming unusually secretive about their screen or quickly switching tabs when you walk by.
- Unexplained withdrawal from family activities, physical friends, or schoolwork.



The Cyber Helpline



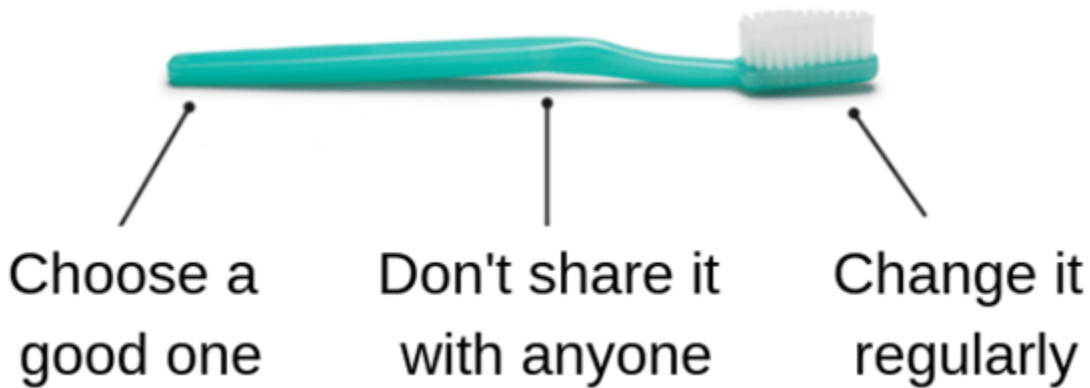
THE "SAFE CROSS CODE" FOR THE INTERNET

Use the **Stop, Think, Check** model.

Step 1: STOP (Immediate Defensive Actions)

The Toothbrush Rule: Teach children that a password is exactly like a toothbrush—it should never be shared with friends and must be changed regularly.

A password is like a toothbrush

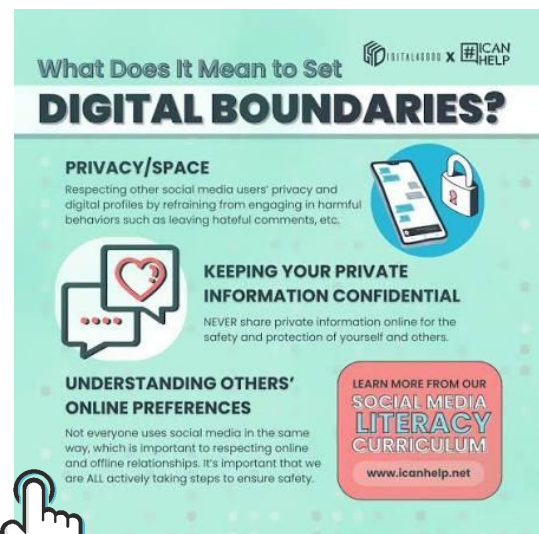


Account Locking: Transition every social media profile and online gaming account to strict **Private Mode**. Never accept friend requests from individuals who are not known in the real world.



Step 2: THINK (Critical Evaluation)

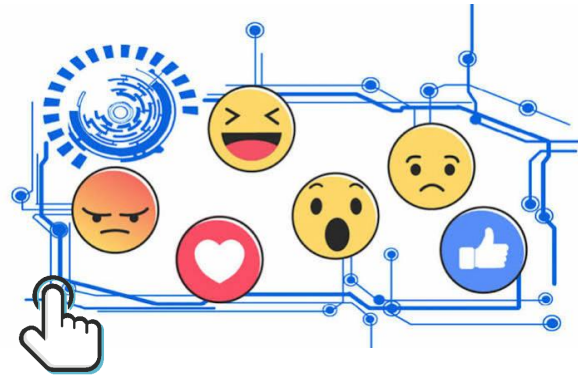
Data Boundary Rule: Never enter a home address, school name, telephone number, or parent's workplace into an online prompt, app registration, or public forum.



The Reality Check: Remember that online avatars can easily be faked. An AI chatbot is not a real friend, and a peer online might not be who they claim to be.



Digital Empathy: Apply real-world kindness rules online. Do not post, share, or forward comments that mock, exclude, or hurt another person.



Step 3: CHECK (Mindful Verification)

Unfollow Toxic Elements: Audit feeds regularly. If a profile, influencer, or account triggers feelings of sadness, inferiority, or anxiety, unfollow it immediately.



Verify Prior to Action: Slow down. Check information accuracy with a trusted source before clicking links, sharing posts, or attempting to buy in-game items.

Report and Disengage: If an online interaction feels unsafe, mean, or inappropriate, turn off the screen immediately. Tell a trusted adult right away, then block and report the account.





3 Small Ways to Teach Your Kids Digital Empathy



ACTION PLAN

A passive approach to internet safety is ineffective. Safeguarding requires concrete physical, technical, and conversational strategies.

Technical Device Interventions

Router-Level Filtering: Install age-appropriate filters on home Wi-Fi routers to block access to explicit websites, adult imagery, and known malware networks.



Onboard Operating System Controls: Configure Apple Screen Time or Google Family Link to require adult approval for all app downloads, block in-app purchases, and automatically lock down devices during sleeping hours.

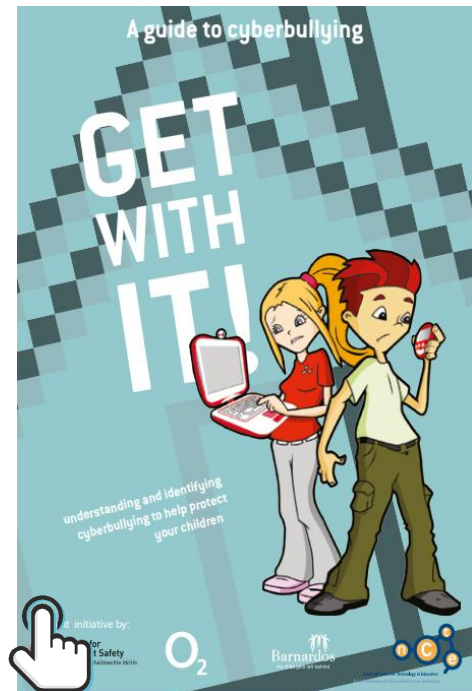


Bedroom Device Ban: Establish a firm household rule that all smartphones, laptops, and tablets are charging in a central communal space overnight, removing screens from private bedrooms.



Communicative & Institutional Safeguards

Establish a Judgment-Free Zone: Children often hide instances of cyberbullying or online grooming because they are terrified adults will confiscate their phone. Reassure them that their access will not be punished if they report an uncomfortable interaction.



School & Institutional Policies: Educational professionals must formulate clear Digital Acceptable Use Policies (AUPs). These rules should cover smart device

limitations during school hours, peer-to-peer digital respect, and structured media literacy training.



RESOURCE DIRECTORY

Organisation	Core Services Provided	Official Portal
Webwise	Classroom learning toolkits (<i>HTML Heroes / Connected</i>); explicit guidebooks for configuring individual app settings.	webwise.ie
Barnardos	<i>Level Up</i> workshops for school environments; dedicated support documentation addressing social media burnout.	www.barnardos.ie
CyberSafeKids	Interactive cyber-safety audits; corporate and school informational talks; "First Smartphone" evaluation checklists.	www.cybersafekids.ie
ISPCC / Childline	24/7 therapeutic support line for minors; professional support guides managing online grooming and sexting fears.	www.ispcc.ie
Internet Matters	Step-by-step downloadable PDFs detailing how to configure parental locks on specific tech products and consoles.	www.internetmatters.org
NSPCC	From understanding apps to setting parental controls, we've got information and resources to help you understand online safety and talk about it with children and young people.	https://www.nspcc.org.uk/keeping-children-safe/online-safety/
Unicef		https://www.unicef.org/parenting/child-care/keep-your-child-safe-online
Coimisiún na Meán		https://www.cnam.ie/general-public/children-young-people/keeping-safe-online/
Data Protection Commission	"Pause Before You Post" Awareness Campaign	https://www.dataprotection.ie/en/children

DCU Anti Bullying Centre	The DCU Anti-Bullying Centre, a leading international research centre advancing knowledge, policy, and practice in the fields of bullying, cyberbullying, and online safety.	https://www.dcu.ie/antibullyingcentre
Tackle Bullying	Tackle Bullying is a national website to counter bullying and cyberbullying for young people, parents and teachers. The site is funded by the Department of Education and Youth under the 2013 Action Plan on Bullying (2013) and provides a single point of contact for those who are affected or concerned about Bullying and Cyberbullying-related incidents, giving access to the most up-to-date research and support in the areas of bullying and cyberbullying.	https://tacklebullying.ie/
Tozi App	Tozi is a new app, created by the Vodafone Foundation in partnership with DCU Anti-Bullying Centre and Childline by ISPCC. Tozi was designed to empower young people and their communities to navigate the online world in a safe and positive way.	https://www.to-zi.com/
Zeeko	At Zeeko, our programmes are designed to strengthen digital education, helping schools, teachers, parents, and students adapt to the ever-changing online world. We provide engaging Internet Safety Seminars , practical classroom resources, and innovative tools such as our Digital Trend Report and Report Card Generator , which help schools track and respond to digital behaviours. To further support	https://zeeko.ie/cyberbullying-in-digital-world-growing-problem/

	digital learning, we supply the Phoenix Quest 10 Notebook PC , designed specifically to empower students as confident and creative digital learners.	
5 Rights Foundation	As an international NGO working with and for children for a rights-respecting digital world, we focus on driving change to revolutionise the online environment for children and society as a whole.	https://5rightsfoundation.com/
Children's Rights Alliance	The Children's Rights Alliance unites over 150 members working together to make Ireland one of the best places in the world to be a child. We change the lives of all children in Ireland by making sure that their rights are respected and protected in our laws, policies, and services.	https://childrensrights.ie/wp-content/uploads/2025/04/Online-Safety-Monitor-2025.pdf

For Kids & Teens (Young People)

The internet is a vast space for learning and connecting, but protecting your personal data and well-being requires specific digital habits.

Protecting Personal Privacy

The "Billboard Rule": Never post text, photos, or videos that you would be embarrassed to see displayed on a giant billboard outside your school or house.



Lock Down Data: Keep your full name, home address, phone number, school name, and current location strictly private. Never share these in public chats or bios.

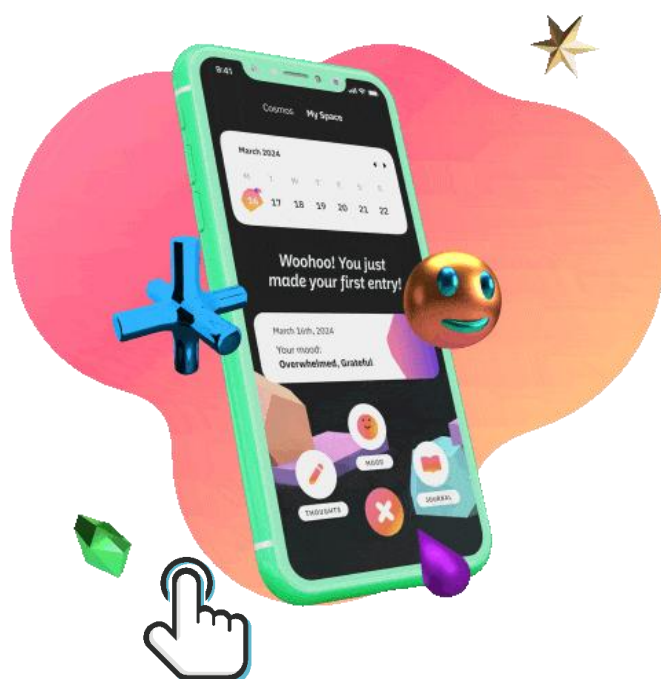
Secure Logins: Use strong, unique passwords for every account. Never share passwords with friends, classmates, or online partners.

Stranger Danger is Digital: People online are not always who they claim to be. Never agree to meet an online-only acquaintance in person without a parent's permission and supervision.



Navigating Social Spaces

Treat Others with Respect: Avoid typing things you wouldn't say to someone's face. Cyberbullying hurts just as much as physical bullying.



[Download TOZI on IOS here](#)

[Download Tozi on Android here](#)

Use the Block and Report Features: If someone is bothering, threatening, or harassing you, immediately use the platform's built-in tools to block them and report their profile.

Take Screenshots: If you experience online harassment, save screenshots as evidence before the messages can be deleted or altered.

Trust Your Gut: If a conversation, photo request, or link feels strange, uncomfortable, or scary, close the app immediately and tell a trusted adult.



Trusted Online Safety Organisations

For deeper reading, template agreements, and step-by-step technical guides, consult these dedicated platforms:

- [Webwise](#): Offers comprehensive Irish internet safety advice, conversation starters, and specific breakdowns on emerging tech like generative AI.
- [Tusla \(Child and Family Agency\)](#): Provides parental PDF guides regarding digital safety, developmental advice, and setting boundaries.
- [CyberSafeKids](#): An organization focusing on empowering children and parents to navigate the digital world safely through school talks and downloadable resources.
- [ConnectSafely](#): A global non-profit providing clearly structured, platform-specific safety guides for parents concerning popular apps and games.

Kid Friendly Social Networks

If your child is eager to start tweeting, posting or sharing but you feel they're not ready to use the likes of Snapchat or Instagram, then there are a number of alternative



social networks made for children that you can point them to.

These offer child-friendly features like games and contests but also give you a chance to use them as teaching tool to get them sharing safely.

Ultimately, these social networks give children a safer environment where they can share their experiences and engage with friends they know.



[Kinzoo Messenger](#) is a family- and child-friendly messaging

app that uses wifi rather than a mobile number. It lets users make video calls and share pictures, text and videos with chosen family and friends.

Safety features

- It does not use persuasive design to keep children using the app, which can help children take breaks.
- The community is limited to your child's family and friends rather than a global community.

Age: 6+

Cost: Free

Available on: [Android](#) and [iOS](#)





Liaura is a guardian-managed digital community built specifically for children aged 6 to 11. It uses safeguarding-first design and input from educators, safeguarding specialists and community

organisations. This helps to provide a structured digital space to help children build confidence.

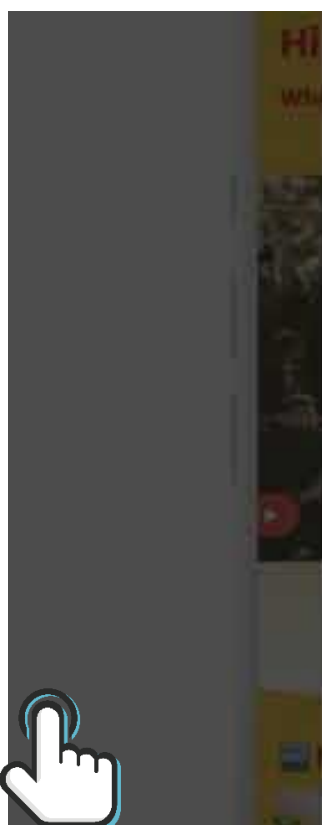
Safety features

- A community for primary-aged children that is managed by parents or carers.
- No open feeds or content discovery driven through algorithms.
- Community spaces are structured and moderated with controlled enrolment.
- Parents and carers have a view over participation with and connections to others.
- No advertising feeds or monetisation of children's data.

Age: 6-11

Cost: £2.99/month (with 90-day free trial)

Available on: [Android](#) and [iOS](#)



Play with purpose.
Learn for life.





zigazoo

Zigazoo is the world's largest social media platform for kids. It's designed with safety, education and fun at its heart.

Often described as a kid-friendly alternative to TikTok, the app lets children create and share short-form videos in response to daily challenges from celebrities, brands and creators. Interactions on the platform are built to promote positivity, creativity and digital citizenship.

Safety features

- A kids-only community, verified with [age assurance technology](#).
- Media is screened to ensure it's developmentally appropriate.
- Parents must sign up their child using their own email to verify children's accounts.
- Options and oversight for which communities your child joins.
- There are options to share privately or publicly.
- Features for interaction are designed to promote positivity and build confidence.

Age: 5+

Cost: Free with in-app purchases

Available on: [Android](#) and [iOS](#)

