Proudly supported by the HSE

CYBERSAFE KIDS

Essential Digital Parenting

A commonsense approach to parenting online lives

EVOLVING GUIDANCE FOR AN EVER-EVOLVING WORLD

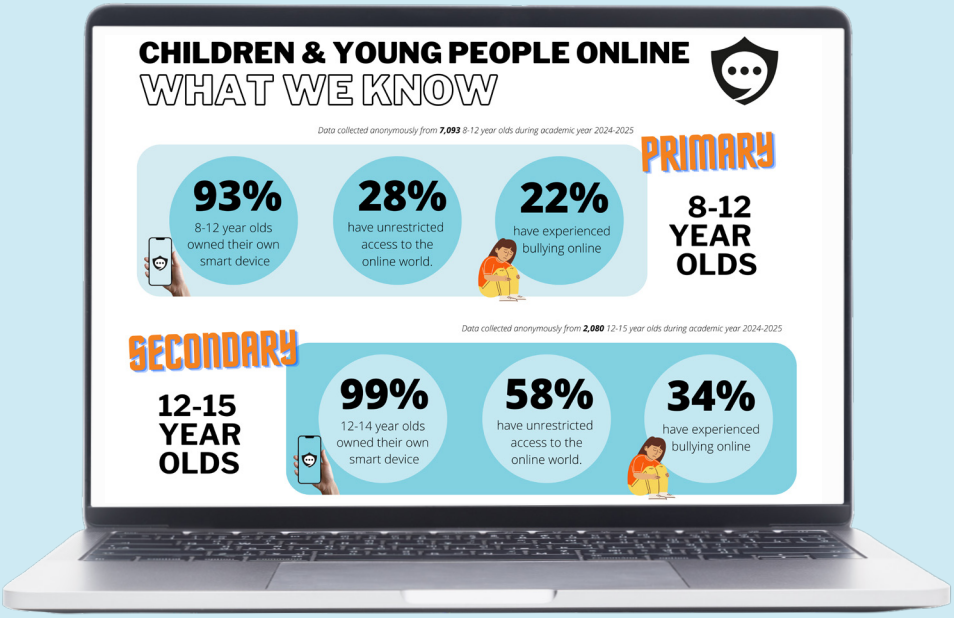
Part of the SAME RULES APPLY campaign

accenture

A Very Warm Welcome...

Welcome to **Essential Digital Parenting**, our latest parenting resource. It is deeply concerning that the world's richest man is using his wealth to enable technology that 'nudifies' women and children on X, rather than investing in tools that protect them. The need for action has never been greater. After the continuing success of Same Rules Apply, this new, updated booklet for 2026-27 is a key part of our annual parental awareness campaign, now in its fifth year. Once again, it has been created with the generous support of the HSE and Accenture. The booklet has been refreshed to reflect the ever-evolving online world, and is aimed at supporting you as parents and caregivers to navigate the often choppy waters of children being online. As always, it is filled with practical tips and useful resources that we hope will help steer you in the right direction, and give you confidence to support your children's online lives more effectively. While 2025 has seen many successes, we still have a long way to go, and there is still much work to be done to make the online world safer for children.

Alex Cooney, CEO, CyberSafeKids



What is 'Digital Parenting'?

Whether we like it or not, it's a reality of modern parenting that children are often referred to misleadingly as 'digital natives'. While that may be true, being born into a digital age does not mean they are inherently born with the skills to function safely and effectively within it. We were all born into the age of the automobile, but we still had to learn how to drive, right?! Approaching children's online lives with the same care, attention and supervision that we apply to their offline lives is vital: always remember that ***when you give your child access to the online world, you are also giving the online world access to your child.***

Very young children should never access the internet alone: they should be supervised at all times. It can be easy to access inappropriate content without intending to.

As children mature, they will inevitably want more privacy but it's essential to continue to regularly monitor and supervise their online activity in an atmosphere of trust and transparency, including checking devices and apps for inappropriate content and contacts.

While challenges or harms in the online world vary from age to age, ongoing dialogue and discussion around the online world is essential regardless of age. Discussing online life as a normal part of everyday conversations is the only way to keep your children safe and ensure their experiences online are as positive as they can be. With that in mind, let's dive in...

Contents

Getting Started: Introducing Technology

As parents you may feel overwhelmed about how to protect your children from *the risks* of being online, but it's important to acknowledge *the benefits*: having fun and socialising, or learning and developing creative skills.

Providing support by guiding your child safely means they are less likely to go online secretly and access inappropriate content, unwittingly or not.

Talk with your child in an age-appropriate way about some of the important things to watch out for when going online.

Have them think about who they talk to online.

Talk about how they should behave online (in the exact same way as you'd hope they behave offline!).

Supervise them at all times when they are young and first exploring the online world.

Introduce devices and online platforms (social media & gaming) slowly and carefully.

Getting Started: Developing Healthy Habits

Think ***quality not quantity***. Children need clear guidelines and boundaries. Screen time encompasses almost everything we do in our daily lives, and if you have set a time limit for each day – what is included? Their homework? What about talking to grandparents in another town or country?

Children might be doing something creative online, so ***focus on the activities and achieving the right balance,*** rather than focusing solely on the amount of time spent on screens.

- ***Agree rules*** about the different types of online activities.
- Talk about ***when*** and ***where*** it's appropriate to use screens (ideally, keep devices out of bedrooms, especially overnight!)
- ***Agree times*** when screens are and aren't allowed in the home (meal times and bedtime may be a good start to the not-allowed list!).
- ***Model the behaviours*** you want to see yourself.
- Think not just about the quantity of screen time but rather the ***quality of activities*** your child may engage in.
- Minimise time spent doing passive, sedentary activities like scrolling or mindless gaming.

Getting Started: *When should I buy my child a smartphone?*

This is a question we hear a lot, and you're not going to like the answer...*it depends*. Every child is different and you know them better than anyone else, so only you can really know the best age. Ask yourself, is your child ready to take this responsibility on and are YOU ready for the responsibility that comes with it? The last 12 months have seen much talk about smartphone 'bans' and social contracts, but the reality is more complicated. We would encourage you as parents and guardians to hold off for as long as possible on getting your children a smartphone. Whatever you decide, here are some useful things to think about when figuring it out:

- *What is the smartphone primarily being bought for?* (Safety? Gaming? Calling friends & family?)
- *Could you introduce a smartphone in stages?* Start with an alternative that provides basic connectivity with limits on social media and web browsing (e.g. from old style Nokia to Phone+, Light Phone, Balance Phone, Pinwheel)
- *Have you agreed rules of use?* (e.g. What can be accessed? Can apps and games be downloaded?)
- *Have you done your research on parental control apps available on Apple or Android?* (See p.8 / p.27)
- *Are you prepared to keep monitoring its use, and apply sanctions if necessary?*

Please Remember!

Talking only about *smartphones* can be a red herring. Our research shows that tablets and gaming consoles are consistently the two most popular devices among 8-12 year olds (smartphones are third), and although they might be used more generally in the home, both harmful content and contact can be encountered just as easily on these kinds of devices, so monitoring and supervision are still essential.

You can build a community of schools and parents across Ireland, to support delaying access to smartphones and social media. One of these is Smartphone Free Childhood Ireland.

Staying Safe & Private: Using Parental Controls

Most smart devices and online platforms have built-in controls that allow you to limit time, restrict access to certain content, and switch off functions like direct messaging, chat rooms or shopping.

- Both Apple and Android have ***family management systems*** built-in to monitor individual devices.
- ***Filtering controls*** on devices and WiFi routers are useful for preventing children from accidentally encountering harmful content.
- Minimise the risk of inappropriate content by ***activating safe search options*** in your browsers.
- Make use of the ***built-in parental controls*** for apps and games, such as paired accounts, content filters, or screen-time limits.
- Many apps and games give their users the option of buying a host of extras and children can easily make purchases (sometimes without even realising). ***Disable in-app purchases*** using your phone or device settings.
- There are many resources and websites to help, as well as device or console manufacturer's websites.

With so many devices and platforms, ***'How to' videos on YouTube can often be a great place to start*** for all of these: they are just a quick Google search away...

Staying Safe & Private: Setting Ground Rules

Be the best role model for your child.

Modelling behaviour is the most powerful way you can influence your child's behaviour.

If there is a rule about no phones at the dinner table – that means for everyone! Using your phone at the dinner table (is it really that important?) may send very mixed messages.

As parents or guardians, we can justify our use of screens at the dinner table by saying that "it's for work" or "it's important", but what young people are doing online is also very important to them.

› This is really about modelling behaviour, so ask yourself...*can it wait?*

› *Be conscious of how many times you're picking your phone up* and looking at the screen in their presence.

› *Avoid relying on screens to keep your children occupied:* this confuses messaging on healthy habits.

› *There may be different rules* for you as the parent when it comes to internet use, as for adults generally in life: *this must be discussed and explained to children.*

› Focus on *one screen at a time* - that means that if you are watching a movie you put your phone away! If we double screen we are modeling distracted attention, normalising constant stimulus, and weakening the shared experience.

› *Take devices out of all bedrooms*, including your own, charging elsewhere.

Staying Safe & Private: Understanding Age Restrictions

Did you know? The General Data Protection Regulation (GDPR) requires an ***age of digital consent.***

In Ireland, the legal digital age of consent is 16. For data collection, teenagers between the ages of 13 and 16 years old must have parental permission to sign up to social media services.

Most social media platforms and services have a minimum age requirement of 13 years old. ***Children under the age of 13 should not have their own social media accounts.*** However most social media platforms do not have robust age-verifications in place making it easy for underage users to sign up, as borne out by the fact that 70% of 8-12 year olds already have their own social media accounts.*

Sometimes app stores (Apple/Google Play) have their own age rating systems, so it is better to follow standardised guidelines and ratings.

Use ***www.commonsensemedia.org*** or ***pegi.info*** for a comprehensive list of age requirements for social media platforms and games.

A Life Behind The Screens, Trends and Usage Report, CyberSafeKids (Academic Year 2024-2025)

Harms & Risks: Social Media & Gaming

When your child begins using social media, these are the key questions to ask yourself:

Am I comfortable with my child using platforms not designed for children? Ultimately, you need to decide if your child is emotionally equipped to deal with the social pressures that can arise such as 'fitting in' or 'being popular.'

Have I researched the app or game my child wants to access? Take time as a parent to review the app and/or game and decide if it's an appropriate service for your child. Use helpful websites like Common Sense Media, Webwise or PEGI.

Is the profile set to private? In the event of any problems occurring, do you also know the password to gain immediate access, if needed? Check out the platform before agreeing to anything with your child. Is there potential for harassment or accessing inappropriate content?

Do I and my child understand how the platform works, and how to report and manage privacy settings together? It is essential to always report or block problematic contact or content within apps and games.

Why not check out Webwise's useful introductory guide to online gaming for parents? Access the guide by clicking here.

Harms & Risks: Cyberbullying

Cyberbullying is something you should talk about before it happens. It's continuously evolving and can happen to anyone of any age when online.

Cyberbullying can be defined as ***targeting someone deliberately online*** using technology such as social media and gaming platforms, instant messaging apps and websites. It can include:

- Hurtful messages
- Excluding people from groups
- Posting nasty comments
- Using photos or videos of someone without their permission
- Threatening to share things about someone online
- Using fake profiles or accounts to target, threaten or scare someone
- 'Bandwagoning' (getting swept up in the momentum of a group chat)

Cyberbullying does not require face-to-face contact. It can occur 24-7.

Report Problems

Report instances of cyberbullying to online service providers that have reporting tools. By using this reporting mechanism, your child will be passing information on to people who may be able to prevent cyberbullying. If the harassment is severe and ongoing, contact the Gardai ***(Garda Confidential Line: 1800 666 111).***

*If cyberbullying content is of a sexually explicit nature and features images of minors it is important when screenshotting that you ***do not share images (or store them in the Cloud)*** as this can be considered legally as distribution without consent. Secure the device in question, reassure the young person and try and ascertain how far the image(s) may have been shared.

Children need to understand the emotional damage that cyberbullying can cause. Teach empathy skills to your child and emphasise the importance of not standing by while someone else is being bullied. Encourage them to be an 'upstander' rather than a 'bystander'. Remind them that telling a trusted adult is not 'telling tales'.

What Advice Should I Give my Child?

- *Tell a Trusted Adult*
- *Don't Reply*
- *Keep the Messages*
- *Block the Senders*

Harms & Risks: Managing Privacy

Make sure your children understand what different types of personal information exist and what is ok to share (and not to share) online. Many of the most popular social media platforms are set to **public** by default. This means that **everything** a young person posts can be **seen by anyone** unless this setting is changed. Explore **private** or **friends/contacts-only** settings.

It's a good idea to talk about your child's **friends list.** Sometimes, in their desire for popularity, young people become too relaxed about who they'll accept as 'friends'. You and your child should review their list of online 'friends' regularly, so they are sharing their information only with people they trust. It is unlikely that a child knows 300 or more people offline, so they shouldn't have this many 'followers' online!

Emphasise that **children should NOT reply to any unwanted messages.** Although it may seem obvious, scam artists or predators use messages that draw responses from young people. Make sure your child knows how important it is to ignore them and to speak to you if something bad happens, which makes them feel uncomfortable. 'Fun online quizzes' can also be a way for scammers to get children to put more personal information online than they should (or need to).

Cyberthreats through games, including malware attacks on shared devices, are also on the rise so make sure they know not to accept downloads or to share their gaming account details without permission.

Approaching Tricky Topics

Always ensure children understand that sometimes **inappropriate content will find them** – this isn't their fault or something that they'll be reprimanded for but they must come and tell you. Praise your child for coming to you about the problem, stay calm and don't overreact. Make a plan together to try and prevent it from happening again.

Make sure location settings are set to 'OFF'

Location, Location, Location!

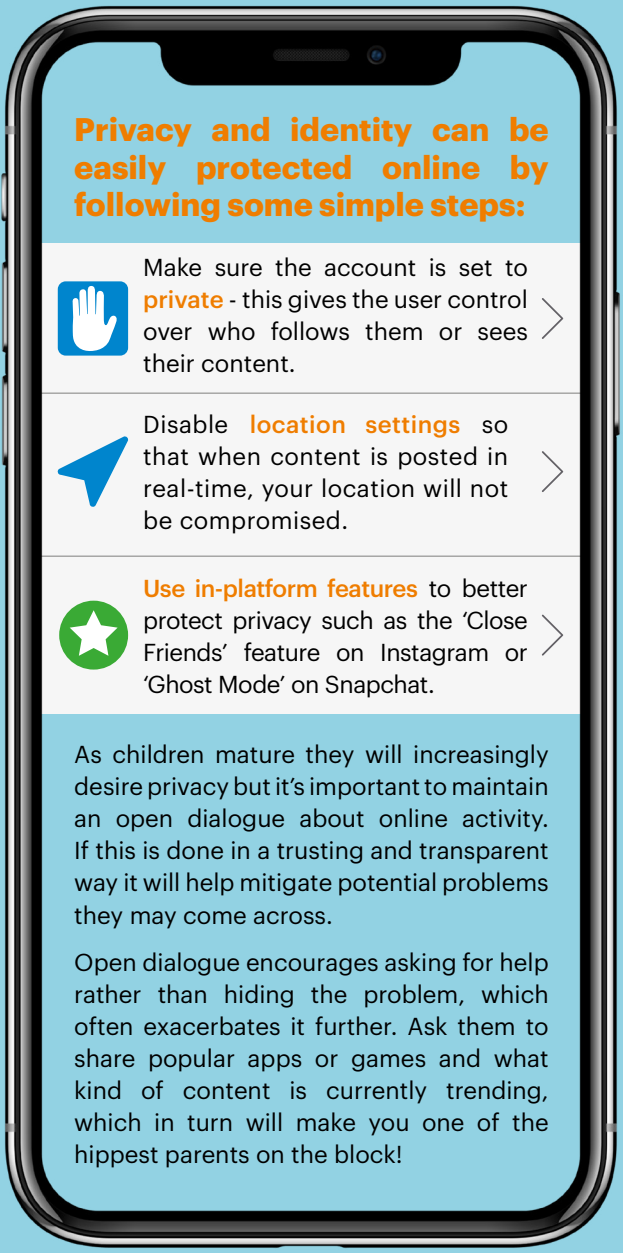
Many apps and platforms will ask for access to your location through GPS tracking. There's never any occasion when anyone other than you should need to know where your child is, so make sure **location settings are set to off** both on the device your child is using and within the specific apps and games they are accessing.

Similarly, turning location settings off means that video and photo content will not be 'geotagged' even if it is posted online, so no information on where or when the video or photo was created can be extracted from the metadata. This is especially important if your child is posting in real-time, for example, taking photos on the beach and uploading them to a social media platform while still in situ.

A Gentle Reminder...

Remember, even if you have strong controls at home, children can still encounter inappropriate content in other settings or on devices belonging to friends or peers, so it is wise to not rely on these solely.

Harms & Risks: Privacy Loss



Harms & Risks: Grooming

The online world can be an easy place for groomers to contact children and young people to develop inappropriate relationships with them. The ease of taking and sending images and videos means that a lot of child sexual abuse material (CSAM) is generated through these kinds of channels. Telling signs this may be happening include:

Listen to Orla's Story here:

- Wanting or asking to ***spend more time on the internet.***
- ***Being secretive*** about the sites they visit or who they are talking to online.
- ***Switching screens*** when you come near them when they are on their laptop, tablet or phone.
- ***Possessing new items*** you haven't given them, especially electronic devices.
- ***Sexual language/imagery*** you don't expect them to know or that is ***not age-appropriate.***
- ***Emotions*** that become more volatile, unexplained distress.

If you suspect a child is being groomed:

- Stay calm, respond positively, reassure them.
- Encourage them to talk openly.
- Advise that they don't respond to or delete messages.
- Use privacy settings, online blocking & reporting mechanisms.
- Talk to the Gardai if involving serious harassment, threat of harm or indecent images or videos.
- Use expert helplines such as Childline.
- Visit ***www.hotline.ie*** for more information.

Harms & Risks:
Sexting & Pornography

15% of 15-17 year olds have received sexual messages online.*

The sending or receiving of any sexual image of a minor by anyone is a criminal offence and young people can fail to recognise privacy and legal concerns. Images leak easily online, and although sexual curiosity and experimentation are a normal part of growing up, it is important to ask the question: ***who will see this in the future?*** The sending or receiving of sexual images - with or without consent - when a minor is involved can have devastating personal, emotional and legal consequences for young people and families. This includes AI generated imagery.

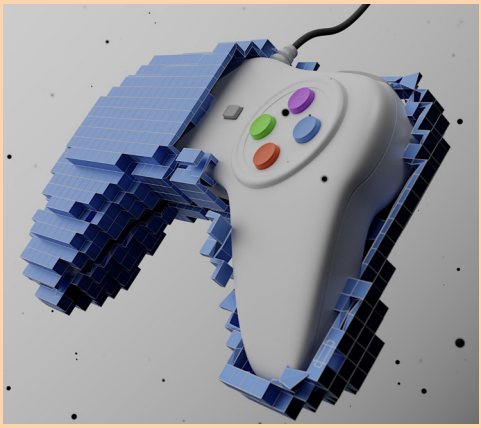
When online, young people are likely to come across pornography and although first exposure is often accidental, research shows that 54% of children see pornography for the first time before the age of 13** – with the average age being 12. Once your child and their peers are active online, it is inevitable they will come across inappropriate content because it's all too easy to access and children are curious. So be prepared. Have the conversation about topics such as porn, consent and sexuality, even though it can be tricky. The key message to get across is that not everything they see is real. This is important, otherwise it can lead to a misunderstanding of what is "normal" behaviour. Check out the New Zealand government's 'Keep it Real' campaign for inspiration on the importance of these conversations!

*Ref: NACOS 2021 Going Deeper: Sexting & Pornography Robb, M.B., & Mann, S. (2023). **Teens and pornography. San Francisco, CA: Common Sense. www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf

Harms & Risks: Gam(bl)ing

Young people can be exposed to gambling through the video games they play, even those aimed at very young children. People who engage in some form of gambling as children are almost twice as likely to have a gambling problem as an adult (2026 ESRI study).

Video games can normalise gambling with casino imagery, betting with virtual currency and randomised purchases (paid loot boxes).



It is important to:

Research popular games young people are playing to assess if they are suitable before playing, e.g. look for warning labels for *Gambling* or *In-game purchases (includes random items)* and casino imagery.

Agree on spending rules and limits up front – less frequent purchasing is better. Try gift cards.	Remove payment details from consoles/ stores or set up spending limits using parental controls.	Monitor behavioural changes around their gameplay, such as increased secrecy or anxiety.

*Childhood exposure increases risk of problem gambling – study. RTE, 2026.

1. Information

The online world is awash with information, much of it increasingly *misinformation* or *disinformation.* It spreads very quickly online so it's imperative that young people develop a healthy scepticism about the information they consume and understand the difference between information that is inaccurate and information that is deliberately designed to mislead. False images and videos (deep fakes) can be created through technological advances to manipulate audiences and it's important to be able to spot these also.

2. Targeting

Most online platforms work through algorithms and the analysis of user behaviour. The more information you put online, the more you will be targeted with specific advertising and content, which can lead to increasingly existing in an online 'echo chamber' of reinforcing (and possibly harmful) content. This can also include unsafe links and websites designed to get more personal or financial information.

Ever Evolving Worlds: Digital Media Literacy

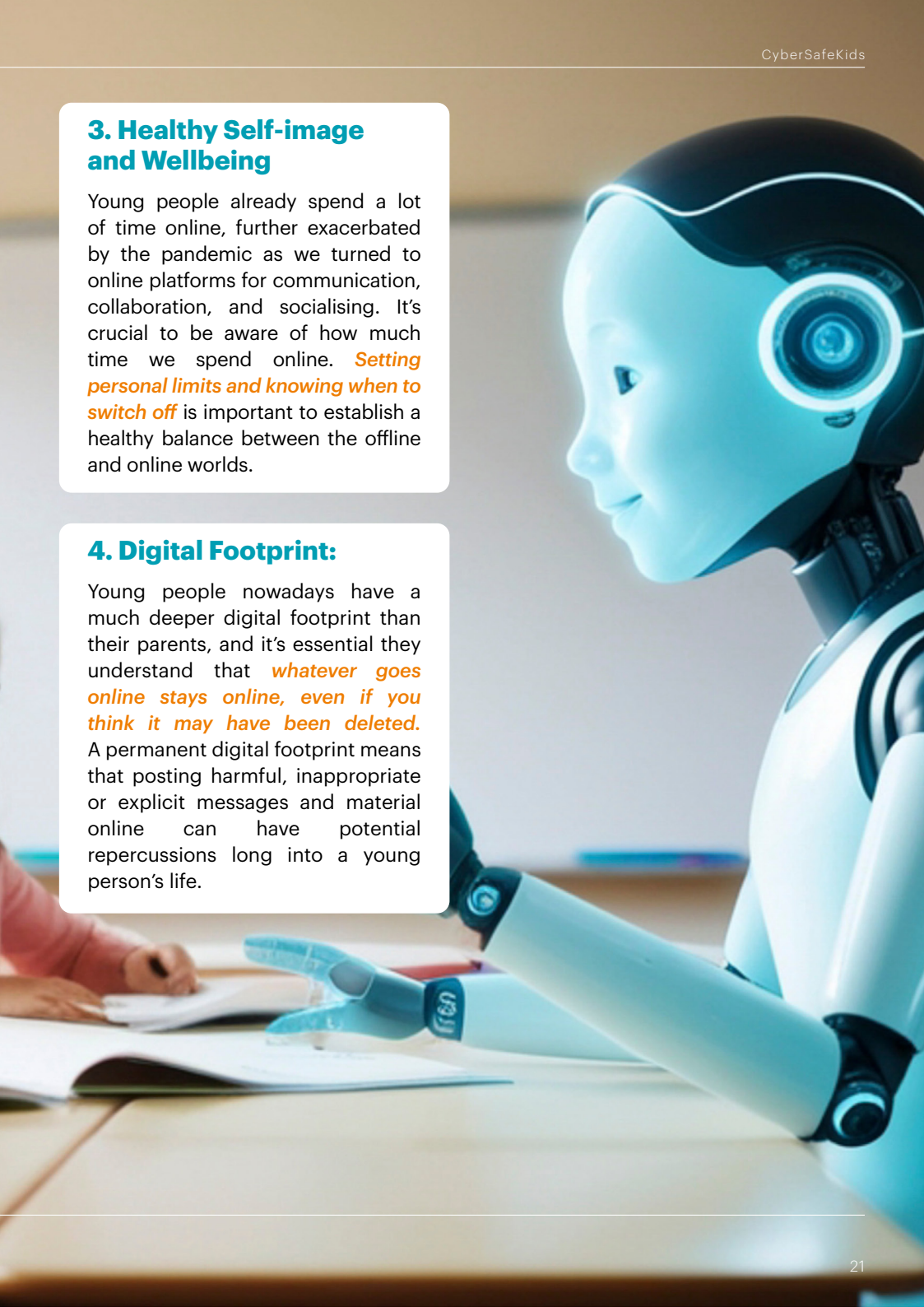
Digital Media Literacy is vital in a visual world where the lines between the offline and online worlds are increasingly blurred. These literacy skills enable young people to think critically, assess and 'read between the lines' when it comes to being online.

3. Healthy Self-image and Wellbeing

Young people already spend a lot of time online, further exacerbated by the pandemic as we turned to online platforms for communication, collaboration, and socialising. It's crucial to be aware of how much time we spend online. ***Setting personal limits and knowing when to switch off*** is important to establish a healthy balance between the offline and online worlds.

4. Digital Footprint:

Young people nowadays have a much deeper digital footprint than their parents, and it's essential they understand that ***whatever goes online stays online, even if you think it may have been deleted.*** A permanent digital footprint means that posting harmful, inappropriate or explicit messages and material online can have potential repercussions long into a young person's life.



Ever Evolving Worlds: *What is misinformation? And disinformation?*

So much information...

While the internet has in many ways democratised information to an extent not seen since the invention of the printing press, it is also, as a result, awash with bad information. More recently, large platforms with global power and influence like X and Meta have been very clear in their intention to step back from the responsibility of fact-checking content their users post online, leaving it instead to users and communities themselves. With so many children accessing non-traditional media sources for news and information, this should be a real cause for concern, and it is more important than ever for parents and educators to develop media literacy skills and a healthy scepticism within children from an early age.

Mis- vs. Dis- vs. Mal-information?

There are different types of bad information online, which originate in different sources with varied intentions. A few definitions can be helpful!

Misinformation

Misinformation is false, inaccurate, or misleading information that is communicated regardless of an intention to deceive. It could also be jokes or satirical posts that are taken seriously, or even false product claims in online adverts.

Disinformation

Disinformation is false or misleading information that is created and/or spread deliberately to deceive, something we have seen increasingly weaponised in political circles over the last decade in particular.

Malinformation

Malinformation is the deliberate publication of private information for personal or corporate rather than public interest, such as intimate image abuse or 'doxxing'. There may also be deliberate change of genuine context, dates or time.

How can my child avoid getting caught out?

There are some very simple habits that can be encouraged to develop these vital media literacy skills:

> Ask yourself: does it seem real? Could it be a joke or satire or even so good/bad/surprising that you want to share

> Check any information for obvious spelling, grammar or translation mistakes (especially email scams!)

> Try and find the same information in other places: look carefully at the source (remember on social media that's the account itself, as you could be watching a deep fake)

> Is the information properly attributed with references listed or is it just someone's opinion?

> Try to balance online sources with traditional/legacy media, e.g RTÉ or BBC

> Read the whole piece and think very carefully before resharing or posting

> Ask yourself whether the information could be AI-generated, and remember that AI-created content can contain errors.

Ever Evolving Worlds: *AI in their Online Lives*

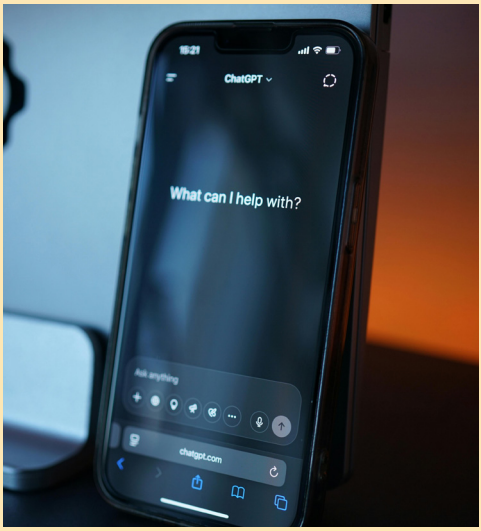
Use of generative AI tools is rising among children, partly because familiar apps like Google Search, WhatsApp, and Snapchat now include AI features. While AI may be beneficial in certain areas of life, with 26% of 8–12-year-olds and 36% of 12–15-year-olds using AI chatbots for school work and advice or companionship*, parents need to be cautious about access, overuse and dependence: it must always be used thoughtfully and critically with adult supervision, rather than being relied on blindly.

Can you trust AI content?

AI makes it easy to publish convincing but false narratives online, including on social media. Chatbots and AI-powered search results can be misleading, drawing on biased, outdated, or incomplete information, and sometimes "hallucinating" answers where data is lacking. As AI increasingly trains on content created by other AI, false or distorted information could amplify. Fact-checking remains essential.

Can ChatGPT do my child's homework?

Relying on AI for answers can undermine problem-solving, critical thinking, and creativity. It also increases the risk of plagiarism. The National Council for Curriculum and Assessment (NCCA) allows AI tools like ChatGPT for research, but AI-generated content must be clearly referenced or it may be treated as plagiarism, a serious offence.



Should AI be their friend?

Nearly 1 in 10 8–15-year-olds use chatbots for advice or companionship*. Children sharing thoughts with AI should know that their inputs can be used to learn about them and may be shared depending on app privacy policies. Frequent use of chatbots as companions may limit real-world social skills. Unlike peers, AI interactions are highly agreeable, offering less challenging and validating experiences.

AI chatbots are not regulated mental health tools. Without safeguards, they may amplify negative thoughts or produce harmful advice. Documented cases include pro-anorexia role-play bots on Character.AI and AI-generated content such as suicide notes on ChatGPT.

A Life Behind The Screens, Trends and Usage Report, CyberSafeKids (Academic Year 2024-2025)

What risks do "nudify" and AI identity misuse pose?

AI nudification features are widely accessible, via "nudify" apps or through chatbots that enable images uploaded to be undressed and manipulated. Children's images can be manipulated or shared to humiliate them. AI-generated content can be used for sextortion scams, and voice cloning tools can create audio clips from just 15 seconds of online recordings.

Sharing images of children, even before they have accounts ("sharenting"), increases the risk of misuse. 90% of AI-generated CSAM* is now indistinguishable from real content**, and production of extreme "Category A" material is rising. Deepfake videos and fine-tuned AI models can generate nearly any image or video of a child. Generating or sharing non-consensual intimate images, including AI-generated, is illegal and should be reported to An Garda Síochána and Hotline.ie. More information for parents and schools can be found from Webwise.

Tips to reduce risks when using AI!

> Fact check AI outputs: Encourage children to verify important information with reliable sources, especially for schoolwork, since AI is not always accurate.

> Use AI to support learning, not replace it: Chatbots can explain ideas or suggest sources, but children should not rely on them to complete assignments. AI use must always be acknowledged to avoid plagiarism.

> Avoid oversharing images and videos: Public content can be manipulated by AI for bullying, harassment, or scams. Discuss serious consequences of sharing or altering images without consent, even "as a joke".

> Be cautious with AI advice and companionship: Explain that AI chatbots are not people and can give inaccurate or harmful guidance. Children should seek emotional support from trusted adults.

> Set boundaries and check age limits: Use parental controls, limit AI use, and check age ratings and terms. Some AI tools, like Character.AI, are 18+, and companion chatbots may appear in apps children already use, such as Roblox.

> Check privacy policies: Understand how chatbots use, store, or share information generated during interactions.

*Child Sexual Abuse Material **Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery, Internet Watch Foundation, 2024.

Parental Resources: The Law

Coco's Law (Harassment, Harmful Communications and Related Offences Act 2020) criminalises the non-consensual distribution of intimate images (including those generated by AI). This means that either the distribution or publication of intimate images without consent and with intent to cause harm, or even distribution and publication with no specific intent to cause harm, can result in financial penalties and/or imprisonment.

2023 saw the welcome establishment of the ***Office of the Online Safety Commissioner*** in Ireland under the auspices of the Online Safety & Media Regulation Act 2022 and Coimisiún na Meán. This office is responsible for developing online safety codes to make digital services accountable for how they protect people, especially children, from harm online. The Commissioner will enforce rules about how online services deal with illegal or harmful content and will be responsible for carrying out investigations and issuing fines for those companies that are operating in breach of safety regulations.

At a European level we have the Digital Services Act (DSA, 2022). The act "will make sure that all digital services we use, especially the so-called "Very Large Online Platforms" like Instagram, Snapchat, TikTok, YouTube and "Very Large Online Search Engines" like Google or Bing, do more to protect users' rights, keep us safe and stop the spread of illegal or inappropriate content. The DSA covers different types and sizes of online services, used by anyone in the European Union, wherever the service is based. It sets stricter rules for the biggest services".*

We also have the EU's Artificial Intelligence (AI) Act (2024), which is a regulatory framework for AI systems developed or deployed in the EU. Ireland has nine national public authorities responsible for upholding our rights under this act, which includes Coimisiún na Meán, the Ombudsman for Children and the Data Protection Commission.

These EU laws will be complemented by the upcoming Digital Fairness Act, which is still under development. It aims to protect users and especially children from manipulative online practices (including addictive design features, "dark patterns", misleading influencer marketing and personalisation that exploits vulnerabilities.

*REF: The Digital Services Act (DSA) explained, European Commission, 2023.

Ireland's Online Safety Code

Coimisiún na Meán published the first iteration of the Online Safety Code in 2024. Part A obligations were to be met by November 2024 and Part B by July 2025, for those affected. According to the Commission, "The Code sets binding rules applying to video-sharing platforms who have their EU headquarters in Ireland" and they "will take a supervisory approach to enforcing the Code, ensuring that platforms implement appropriate systems to comply with the provisions." *

What exactly is it?

For the first time in Ireland there are now obligations on video-sharing platforms (VSPs) under the jurisdiction of the Irish state to protect people – especially children – from harmful video and associated content. The 9 designated platforms are Facebook, Instagram, YouTube, TikTok, LinkedIn, X, Pinterest, Tumblr, and Udemy.**

> Prohibiting the uploading or sharing of harmful content on their services including cyberbullying, promoting self-harm or suicide and promoting eating or feeding disorders as well as incitement to hatred or violence, terrorism, child sex abuse material, racism and xenophobia.

> Using age assurance to prevent children from encountering pornography or gratuitous violence online and having age verification measures in place as appropriate.

> Providing parental controls for content which may impair the physical, mental, or moral development of children under 16.

Can I make complaints to Coimisiún na Meán?

Not exactly! You can approach the Contact Centre***, but when you encounter harmful content online, first and foremost, ***you should still use the reporting mechanisms on each individual platform.*** This means the platform now has a legal obligation to deal with your complaint in a timely manner. If this does not happen, you can register your complaint with Coimisiún na Meán's Contact Centre, but remember that they are *not a content moderator nor appeals body for the decisions of platforms on individual pieces of content.*****

You can access further information ***here***. Coimisiún na Meán will supervise compliance with the Online Safety Framework, so this kind of information from users about experiences is still very helpful and could lead to significant fines (up to €20 million or 10% of revenue) if systemic failures are detected. As one part of Ireland's Online Safety Framework, the impact of the Code will be assessed on an ongoing basis and revised accordingly. It will be enforced alongside the EU-wide Digital Services Act (DSA) (see p.26).

Watch this useful explainer video about your children's rights to find out more.

*Coimisiún na Meán adopts final Online Safety Code, October 2024 **It is important to note that Snapchat is UK-based and as such, is subject to UK legislation, not Ireland's Online Safety Code or relevant EU regulation (such as the Digital Services Act).
***usersupport@cnam.ie / 01 963 7755 (Monday-Friday, 8am-6pm) ****Revised Online Safety Code Q&A – 21 October 2024

Parental Resources: Developing a Family Agreement

Bear in mind that children with less parental supervision and more online access are more vulnerable to risks online, especially when they are young so...

› Normalise discussing their online activity on an ongoing basis, without judgement.

› Do your research, set rules, time limits and clear boundaries and stick to them for example, no phone usage is allowed between 8pm - 8am. Keep smart devices (mobiles, laptops, tablets, gaming consoles) downstairs overnight.

› Use devices in open spaces, not behind shut doors, unsupervised.

› Encourage phone-free rooms, e.g. no phone is allowed in the bedroom.

› Use the 'one screen at one time' rule, rather than watching TV while also on another device.

› Use technical restrictions (such as parental controls) but don't rely on them alone, especially when expectations of privacy increase.

› Model good behaviour and encourage healthy habits, like checking your screen time regularly.

› Build a shared community of parents and guardians, teachers and experts.

Parental Resources: Developing a Family Agreement

A family agreement can be a great way to normalise discussing online life.

Creating one as a family and displaying it prominently in the house is a proactive and engaging way to create 'buy-in' from all, and hold everyone to account for their online behaviours and habits.

So how do we get started?

› *Create time to have a conversation* with your family about your online lives – think about how you use the online space and what your habits and behaviours are online.

› *Generate an atmosphere of mutual respect and trust,* necessary if the agreement is going to work. Imposing restrictions from 'on high' will be much less effective!

› *Try to keep the conversation positive:* make the focus on safety and healthy habits and draw parallels with the offline world, e.g. the importance of learning how to cross the road safely, or of learning to drive properly.

› *Try tracking online time in advance of sitting down* (e.g. use Screen Time) and sharing it – it can help everyone see current habits and decide together what should be in the family agreement.

If you're thinking of gifting a device, check out our helpful Gadget Gift Guide first by scanning the QR code or clicking here.

Parental Resources: Top Tips!

Other things to consider when setting up your family agreement:

› What types of information are ok to share, and how to keep information safe.

› What games are ok to download: are they age appropriate and will restrictions be needed for 'in-app' purchases?

› Are there ways we can check if the information we see is accurate?

› Who can we chat with or play with online?

› How should we treat people and what to do if we see someone else being treated badly online?

It should also include a plan of action if your children are bothered by something they've seen online. Reassure them that it's not about punishing them or withdrawing their device. It's always about protecting them and making their experiences positive: that's why it's vital they tell you.

Remember:

When you have had these conversations as a family, draw up the agreement with clear statements and make sure that everyone signs it, although some rules may be different for different ages (yes, that includes you as parents too!). It's crucial to also keep your family agreement on display somewhere prominent in the house – it's no use tucked away in a drawer...

You can find an easy to print and use (or adapt!) Family Agreement template by scanning the QR code or clicking here.

Parental Resources: Useful Links

Alva's World
www.irishexaminer.com/news/ireland/arid-40694744.html

Apple Families
www.apple.com/families/

Be Media Smart
www.bemediasmart.ie

Common Sense Media
www.commonsensemedia.org

CyberSafeKids Gadget Gift Guide
www.cybersafekids.ie/giftguide/

Childline
www.childline.ie

Digital Services Act
www.digital-strategy.ec.europa.eu/en/policies/digital-services-act

eSafety Commissioner (AUS)
www.esafety.gov.au/educators

Family Sharing (Apple)
www.support.apple.com/en-gb/guide/personal-safety/welcome

Google Family Link
www.families.google/intl/my/familylink/

Irish Internet Hotline
www.hotline.ie

Keep It Real Campaign (NZ)
www.keepitrealonline.govt.nz

Media Literacy Ireland
www.medialiteracyireland.ie

National Parents Council
www.npc.ie
Call the NPC Helpline: 01 887 4477

ISPCC
www.ispcc.ie/digital-ready-online-safety-supports/

Online Safety Commissioner
www.cnam.ie/online-safety/

Parentline
www.parentline.ie
Phone (01) 8733500
(NI) 0808 802 0400

PEGI
www.pegi.info

Qwant Junior Child-Friendly Browser
www.qwantjunior.com

Same Rules Apply
www.cybersafekids.ie/samerulesapply

Spunout
www.spunout.ie

Trend Micro Cyber Academy
www.trendmicro.com/internet-safety/for-kids/cyber-academy

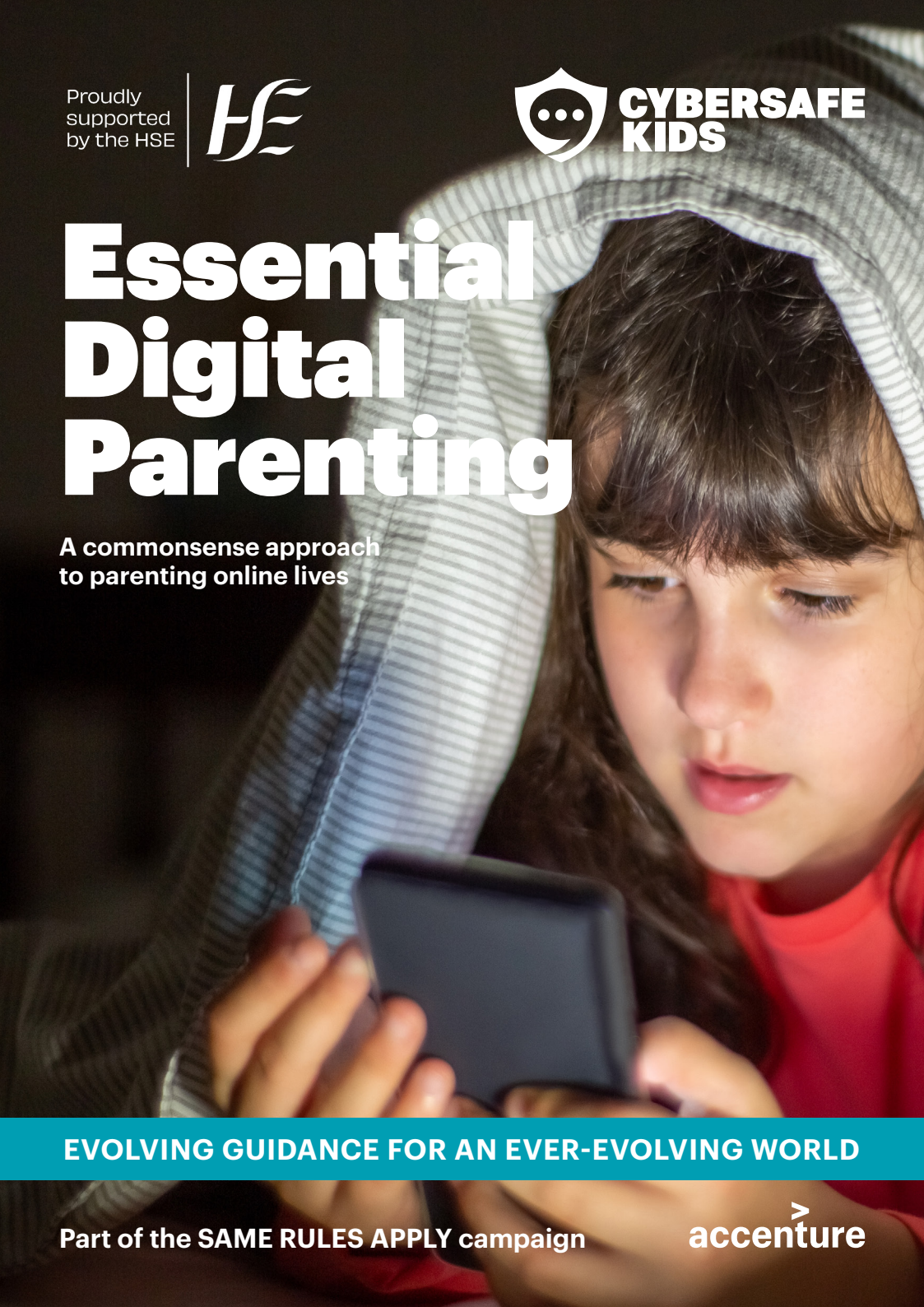
Webwise
www.webwise.ie

Proudly supported by the HSE

CYBERSAFE KIDS

Essential Digital Parenting

A commonsense approach to parenting online lives



EVOLVING GUIDANCE FOR AN EVER-EVOLVING WORLD

Part of the SAME RULES APPLY campaign

accenture