
ONLINE SAFETY AND DIGITAL WELLBEING

An introduction to online risks and
protecting students.



ONLINE SAFETY RISKS- 'THE 4 C'S'

Content

- Violence
- Hate Speech
- Pornography
- Embedded Marketing

Conduct

- Bullying
- Sexual exploitation
- Gambling
- Deepfakes & AI

Contact

- Harassment
- Grooming
- Ideological Persuasion
- Misuse of personal data

Contracts

- Terms of service
- Security
- Data protection
- Online transactions

Figure 2: The 3Cs of online risk (UNICEF, 2017)

Content risks: Where a child is exposed to unwelcome and inappropriate content. This can include sexual, pornographic and violent images; some forms of advertising; racist, discriminatory or hate speech material; and websites advocating unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.

Contact risks: Where a child participates in risky communication, such as with an adult seeking inappropriate contact or soliciting a child for sexual purposes, or with individuals attempting to radicalize a child or persuade him or her to take part in unhealthy or dangerous behaviours.

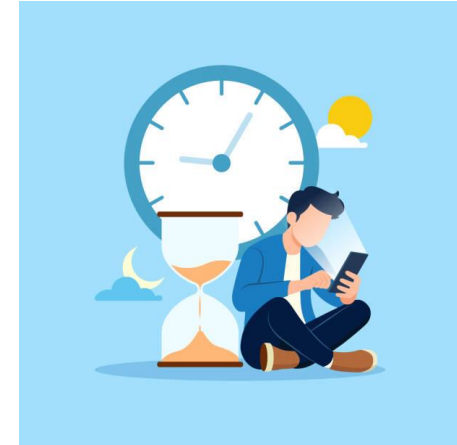
Conduct risks: Where a child behaves in a way that contributes to risky content or contact. This may include children writing or creating hateful materials about other children, inciting racism or posting or distributing sexual images, including material they have produced themselves.

(Livingstone & Stoilova, 2021)

WHAT CAN PARENTS DO?

Screen Time

- Check your child's screen time.
- 2 hours daily is the recommendation for recreational screen time.
- Introduce screen time limits for social media apps and/or games.
- Have an open discussion about screen time and 'doom scrolling'.



How to set screen time limits
(iPhone/iPad)

WHAT CAN PARENTS DO?

Technical controls

- Apps can be used to limit access on devices (see garda document).
- Turn off Bluetooth and AirDrop when not needed.
- Limit purchases in app store settings.
- Apply 'Google Safe Search' on web browsers.



WHAT CAN PARENTS DO?

Active and Open Discussions

- Speak to your child about the risks online. (4 C's)
- Set clear boundaries, limits and rules. Apply sanctions.
- Learn about the apps and websites they like to use.
- Frame the device as a responsibility not just a luxury. E.g. Revolut, contracts, safety.
- Allow access only when the child is old enough.

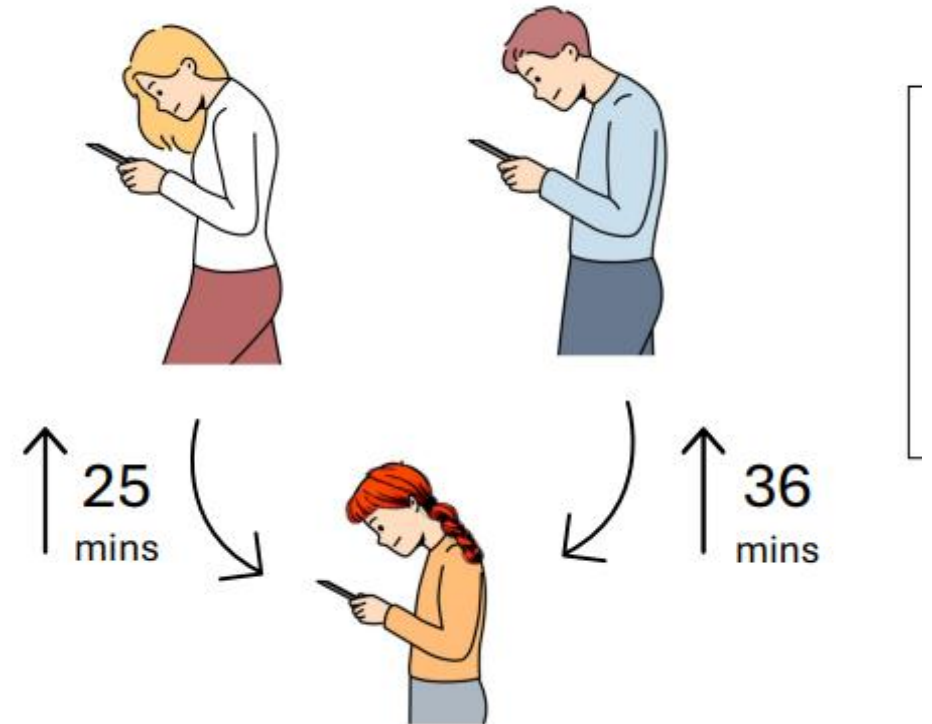


WHAT CAN PARENTS DO?

Reflect on your own device usage.

- Parental screen time has more of an effect on the child's screen time than house rules.
- Parental device usage can disrupt parent-child relationships.
- Lead by example and adhere to your own limits.

For every extra minute of parental social media time



Fox et al., 2025

WHAT CAN PARENTS DO?



Reporting

- Report any illegal or harmful content to Commisiún Na Meán.
- Children have a right to not receive targeted ads.
- These ads, misrepresenting 'influencers', inappropriate material can be reported at www.cnam.ie/reporttous but also always report to the platforms e.g. Instagram, Google, Tiktok

FURTHER INFORMATION



Barnardos
Online Safety
Programme

**Online safety
Webinar
for Parents**



Duration: 45 minutes
Group size: Up to 100
Costs: Free



Barnardos Online Safety Webinars for parents and carers.

Upcoming Dates:

Tuesday 10th February

Wednesday 25th February

Wednesday 11th March

Wednesday 25th March

More dates available

Register at:

<https://www.barnardos.ie/learning-development/training/online-safety-programme/for-parents/>



USEFUL LINKS AND DOCS

- https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf
 - <https://www.cnam.ie/general-public/guides-resources/for-parents/>
 - <https://www.barnardos.ie/learning-development/training/online-safety-programme/for-parents/>
 - <https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/a-parents-guide-to-cyber-safety-small-file-size-.pdf>
 - <https://www.growingup.gov.ie/pubs/8.1-Celine-Fox-Presentation-GUI-2025.pdf>
-