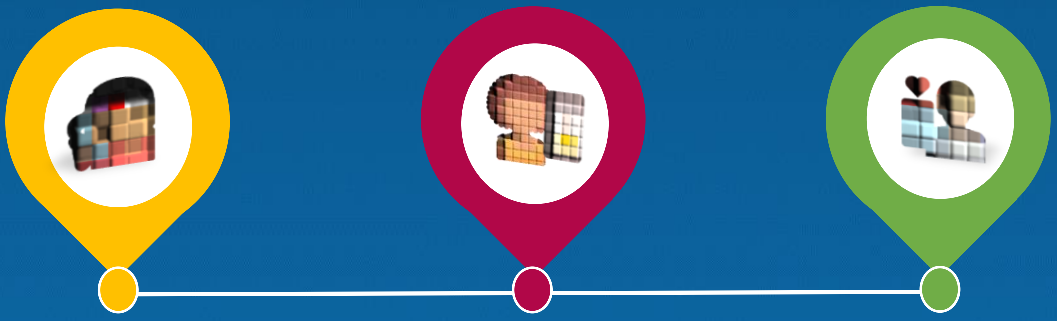
21ST CENTURY CHILDREN:

DIGITAL RISKS AND RESILIENCE

Empowering children to become active and ethical digital citizens requires building capacity to safely navigate the digital world. Digital environments bring enormous opportunity, but also risks. These digital risks can affect children's well-being and undermine their right to privacy.

Education systems have an important role to play in ensuring that children are protected, and learn how to protect themselves, in the digital environment. Age-appropriate interventions must be adapted to children's developing capacity and understanding of digital security and privacy.



5-7 years old

Have a sense of privacy rules but struggle to comprehend the consequences of their actions.

8-11 years old

Privacy is governed more by rules than internalised personality.

12-17 years old

Aware of privacy risks, assess opportunities and risks but tend to focus on short-term benefits when making a decision.

(Livingstone and Stoilova, 2018)

OECD

THE 4Cs:
CONTENT, CONDUCT, CONTACT AND CONTRACT RISKS

Typologies of risks include four broad categories: content, conduct, contract and contact. Many of these are digital versions of traditional risks for children (e.g., bullying, racism and sexism, sexual predation). Just as in everyday life, a zero-risk digital environment is unattainable. However setting the conditions for a safer one is feasible.

CONTENT RISKS

A content risk refers to the child as recipient of harmful, hateful or illegal digital content.

Content risks include:

- pornographic, violent, racist, hateful or generally harmful, age-inappropriate or illegal content
- advertising and spam
- receiving harmful advice or misleading information (e.g., "fake news").

CONDUCT RISKS

A conduct risk refers to the child as actor in a peer-to-peer exchange, including when their own behaviour makes them vulnerable.

Conduct risks include:

- engaging in illegal activity such as downloading or hacking
- bullying or harassing others
- creating or sharing harmful material (i.e. pornography)
- providing harmful advice (e.g., pertaining to suicide, eating disorders).

CONTRACT RISKS

A contract risk (sometimes referred to as consumer-related risk) refers to the child as an active participant in the digital market.

Contract risks include:

- receiving digital marketing messages inappropriate or illegal for children
- being exposed to commercial messages that are not identified as such
- being exposed to economic risk (e.g. digital fraud)
- security risks (e.g., digital scams, identify theft, malicious code).

CONTACT RISKS

A contact risk refers to the child as victim or participant of an interactive encounter.

Contact risks include:

- being bullied, harassed or stalked
- being groomed or succumbing to digital fraud
- tracking or harvesting of personal information; personal data misuse.

OECD

HIGH PRIORITY RISK AREAS

All digital risks can be harmful to children. High-priority cyber risks across OECD countries include :

CYBERBULLYING

- Cyberbullying can be defined as the aggressive targeting of a victim using digital means.
- Many of the mechanisms driving cyberbullying are similar to traditional bullying. Bullies often target their victims both face-to-face and in digital environments.
- The anonymity of digital spaces and the possibility of reaching victims regardless of their physical location differentiate cyberbullying from traditional bullying .

SEXTING AND REVENGE PORN

- Sexting involves creating or sharing sexually suggestive nude or nearly nude images.
- Sexting is illegal if the subject is underage. In severe instances, it can lead to sextortion, where the subject is threatened with exposure if they do not pay a bribe or perform a desired action.
- Revenge porn refers to posting nude images without consent.
- Both revenge porn and underage sexting are illegal in many countries.

SECURITY AND PRIVACY

- Digital activity generates trails of personal data which can be stored on servers around the world.
- Phishing for personal information, surveillance, industrial-scale data processing and behavioural advertising based on personal information are all risks for students.
- It is important to secure and protect children's data and help them understand the importance of digital privacy.

POLICIES AND STRATEGIES TO ADDRESS ONLINE RISKS

Information campaigns and resources

- information and guidelines for parents, teachers and children
- awareness raising activities
- campaigns in partnerships with other community actors.

Teacher support

- resources and pedagogical tools, examples of good practice
- teacher education on identifying and reacting to digital risks
- creation of information materials and training tools.

Child-centred support outside of the school and reporting mechanisms

- reporting schemes for illegal digital activity
- helplines for children, parents and teachers to receive support on psychological, social, legal or administrative processes.

Coordinated policy and frameworks

- elaboration of legal frameworks and/or action plans
- laws , measures and enforcement
- coordination across jurisdictions: the digital world does not respect national boundaries.

BUILDING DIGITAL RESILIENCE

While all children who go online face digital risks, there are some factors that can affect their susceptibility. These include:

- vulnerability: those most at risk offline tend to also be more vulnerable online
- personality factors: sensation-seeking, low self-esteem, psychological difficulties
- social factors: lack of parental support and peer norms
- digital factors: specific digital practices, sites and skills.

Digital resilience refers to having the ability to adjust positively when facing online adversity.

Approaches targeting the household, school and broader levels may contribute to building digital resilience.

HOME

- Target skills of both parents and children to increase their resilience and expand their opportunities. Restricting children's exposure to digital media may decrease risks but also digital opportunities.

SCHOOL

- Train teachers on digital risks and their impacts.
- Foster a zero-tolerance culture to behaviours like cyberbullying.
- Introduce digital ethics and safety learning opportunities in the curriculum.
- Offer spaces for adult and peer mentoring.

SYSTEM

- Create interactive portals with safety tips for children, like the e-safety Kit.
- Create a space for youth to discuss and share ideas on online safety, like the Better Internet for Kids.

ALLIANCES FOR ADDRESSING DIGITAL RISKS: SPOTLIIGHT ON BULLYING

Given the complexities and persistence of bullying both on and offline, there is no easy one-size-fits-all approach to prevent or deal with it. Collaboration among teachers, parents and other members of the community can be part of a good strategy to fight bullying and promote a safe environment for students. Some initiatives include the involvement of external professionals in schools, such as third sector organizations or psychologists, to inform children, parents and teachers about the importance of sympathy, acceptance, patience and respect for the uniqueness of each person.

Key research

- Anderson, E., E. Steen and V. Stavropoulos (2017), "Internet use and Problematic Internet Use: A systematic review of longitudinal research trends in adolescence and emergent adulthood", International Journal of Adolescence and Youth, Vol. 22/4, pp. 430-454, http://dx.doi.org/10.1080/02673843.2016.1227716.
- Kosenko, K., G. Luurs and A. Binder (2017), "Sexting and sexual behavior, 2011-2015: A critical review and meta-analysis of a growing literature", Journal of Computer-Mediated Communication, Vol. 22/3, pp. 141-160, http://dx.doi.org/10.1111/jcc4.12187.
- Livingstone, S. and M. Stoilova (2018), Children's data and privacy online: Exploring the evidence, www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Children's-data-and-privacy-online-exploring-the-evidence.pdf.
- UNICEF (2017), The State of the World's Children: Children in a Digital World, https://www.unicef.org/publications/index_101992.html.

For more, see: Burns, T. & Gottschalk, F. eds. (2019). Educating 21st Century Children: Emotional Well-Being in the Digital Age. Educational Research and Innovation, OECD Publishing, Paris, https://doi.org/10.1787/b7f33425-en.