Digital rights and responsibilities of students and educators

This webinar is designed to support educators to:

- identify the key opportunities and challenges facing children and young people online

- create and facilitate learning opportunities that empower children and young people to develop an understanding of their digital rights and responsibilities

- assist young people to take an active role in protecting and promoting positive and safer online environments for themselves and others.

The program will:

- help to identify the digital rights and responsibilities of educators through a safety lens that extends to the whole community

- examine strategies to communicate and model positive online behaviour.

Section 1
The rights and responsibilities of students

Educators are encouraged to empower students by:

- using a strength-based approach to build digital resilience
- ensuring online safety education is ongoing and integrated
- applying a rights-based approach to strengthen capacity and encourage students to take an active role
- ensuring learning opportunities meet the needs of all students.

This webinar highlights:

- why it's important to know what students think about online safety, and what they see as the risks, opportunities and challenges
- the skills and strategies that young people and children regularly use to self-manage negative online experiences, as reported in eSafety's Mind the Gap research[1]
- the importance of modelling positive behaviours and empowering students with strategies to manage risks (rather than removing problematic content and banning online devices for example)
- the value of social and emotional learning in online safety education, as highlighted in eSafety's Best Practice for Online Safety Education
- the recognition of children's digital rights according to the UN Committee on the Rights of Children

Supporting resources and more information

- Australian Curriculum
- The YeS Project Handout - My worlds
- The eSafety Guide
- eSafety student voice surveys
- Youth aspirational statement
- Children's Commissioner of England and Wales 2018 Who Knows What About Me?

---

[1] eSafety Commissioner (2022). Mind the Gap: Parental awareness of children's exposure to risks online, Aussie Kids Online, Melbourne: eSafety Commissioner

Rights of students

1. The right to feel safe

Children must be given the privacy to act and grow in their own way when they are online[2]. This needs to be balanced with the knowledge that they are more vulnerable to being threatened, receiving unwanted contact and exposing personal information and images.

eSafety commissioned research on the dynamics and impact of technology-facilitated abuse (TFA) involving children in the context of domestic and family violence in 2019-20. Professionals estimated the prevalence of technology-facilitated abuse involving children in domestic and family violence cases at 27%.

This included:

- perpetrators who directly abused children by monitoring or stalking, threatening, intimidating or blocking communication
- children drawn into TFA directed at their mothers who were encouraged by the abuser to facilitate TFA, through gifted GPS-enabled devices and abusive messages sent to their devices[3].

Educators can use structured teaching opportunities to:

- explore the body's warning signs
- practice how to say 'no'
- learn about the technical skills needed to set privacy settings
- explore the responsibility to report
- unpack problematic behaviours
- support students to identify respectful or disrespectful language
- analyse the strategies of others.

Supporting resources and more information

- UN Convention on the Rights of the Child Poster - NAPCAN
- Swoosh and Glide
- eSafety scenarios
- The YeS Project Handout - Crossing the line
- The YeS Project- Decision making wheel
- eSafety reporting abuse portal
- How to report poster
- Young and eSafe (Respect, Resilience, Critical Thinking)
- Play it safe and fair online

[2] unicef.org/child-rights-convention/convention-text-childrens-version
[3] eSafety (2020) Children and technology-facilitated abuse in domestic and family violence situations

2. The right to be heard

Children should be able to say what they think, without spreading untruths or abusing others.[4] Companies and platforms must not push children to do things for money or expose them to content they have not agreed to. The UN General Comment about children's rights in the digital world outlines that processing children's personal data can result in violations or abuses of children's rights.

The responsibility for online safety cannot fall solely on the shoulders of children and their parents, and this is where Proactive and Systemic change can be applied by using Safety by Design.

The risks of being unheard

One in five young Australians aged 8 to 17 years have been socially excluded, threatened or abused online.[5] 45% of young Australians surveyed had been treated in a hurtful or nasty way. Slightly more than a quarter (26%) of surveyed children revealed that they had treated someone in a hurtful or nasty way online in the past year.[6] Severe and prolonged cyberbullying can have long term mental health impacts and lead to self-harm, depression or anxiety. 17% of those surveyed felt their mental health was affected.

Educators can use structured teaching opportunities to:

- support students to understand personalised algorithms and recommender systems
- build awareness of the attention economy
- examine and develop empathy in digital spaces
- develop a clear understanding of online behaviour expectations
- develop awareness of:
  - reporting and support pathways
  - well-being support networks for students.

Supporting resources and more information

- Hector's World
- Activities for students to take the lead in online safety
- Online safety classroom agreement – early years
- Online safety classroom agreement – primary/secondary
- Online safety curriculum connection
- Reset Australia | Policy Memo | TIKTOK: A case study
- Paying Attention: The Attention Economy

---

[4] unicef.org/child-rights-convention/convention-text-childrens-version
[5] eSafety, Youth, kids and digital dangers, 2017
[6] eSafety, Digital lives of Aussie teens, 2021

Section 2
The rights and responsibilities of educators

Staff can experience a range of online challenges including:

- being more accessible after work hours
- the effects of permanent, immediate and wide distribution of reputationally harmful material
- online disinhibition driven by anonymity.

Staff have the right to a safe workplace where:

- schools proactively prevent and respond to online incidents involving staff and all members of the community
- Work, Health and Safety information includes reporting online incidents and escalation pathways
- there is clear communication within the school community about policies, procedures and expectations of appropriate technology-use and respectful communication.

What is adult cyber abuse?

Adult cyber abuse is when someone sends seriously harmful content to a person who is 18 or older, or shares harmful content about them, using an online or electronic service or platform. It can include posts, comments, emails, messages, memes, livestreams, images or videos.

The Online Safety Act defines adult cyber abuse as content targeting a specific Australian adult that is:

- intended to cause serious harm
- menacing, harassing or offensive in all the circumstances.

Supporting resources and more information

- [Professional learning program for teachers](#)
- [Workplace safety guidance (eSafety and Safe Work Australia)](#)
- [Guide to responding to cyber abuse that targets staff](#)
- [Reporting adult cyber abuse](#)

How to communicate positive and safe online behaviour

Communicating to students

- Display digital signage
- Provide session/s led by an eSafety Trusted Provider or a Police Liaison Officer.
- Embed online safety education in all curriculum areas.

Communicating with parents and carers

- Share eSafety's regular blog posts and articles highlighting positive uses of tech by students, or inform parents about trending apps.
- Use the checklist for developing effective online safety policies and procedures to ensure that your ICT capability includes parental behaviour expectations online.
- Proactively upskill parents to support their child's learning and behaviour online.

Strategies for staff

- Include online behaviour expectations and reporting pathways in staff induction and casual relief staff guidelines.
- Have a mentor/buddy system to support shared decision making and debriefing.
- Provide regular online safety PD sessions looking at online trends and behaviours, strategies to mitigate risk, and online abuse.

Digital responsibilities

Self-care responsibilities

Educators are encouraged to use self-care strategies to proactively protect their own wellbeing.

It is important to:

- Build in tech time implications when planning and setting assignments. Avoid including tech elements in every task particularly if it subsequently involves things like discussions boards, moderating chats or additional email communications.
- Create clear boundaries between home and school. You may like to include information in your email signature that states the hours you will access email communications.
- Find a 'debriefing buddy' to brainstorm how to respond. For example, looking at options together if you receive an abusive or emotionally driven email from a student or parent.

Further information
- Online Safety Act 2021