National Student Wellbeing Program (NSWP)
eSafety's Student Wellbeing Officer training webinar notes.
These notes are your quick reference guide.

Preventing and responding to cyberbullying

Cyberbullying trends, challenges and protective factors

What has changed?

Cyberbullying is not new, but the tools, platforms and tactics have become more complex. Here are some of the trends and changes:

- Children are accessing devices earlier, often before they're emotionally ready.
- The use of emojis – for example, sarcastic emojis used to disguise harm as humour.
- Sexualised online abuse behaviours – for example, unsolicited explicit messages, sexual shaming, and threats to share intimate content.
- The use of AI to create fake images, viral, harmful content and to impersonate.
- Chat group behaviours – for example, large chats often become spaces for exclusion, gossip and sharing hurtful content, especially in lower secondary years.

What does it look like?

Cyberbullying in the upper primary years
Bullying often starts face-to-face in peer groups and extends online through messaging apps, games and platforms.

Cyberbullying in the lower to middle secondary years
Bullying becomes more subtle and socially complex, often continuing online through exclusion, gossip and manipulation.

Children and young people with increased vulnerabilities
All children and young people may be affected but there are some who experience a heightened exposure to online abuse, including hate speech, harassment, discrimination and exclusion. They include:

- First Nations children and young people
- children from culturally and linguistically diverse backgrounds
- LGBTQI+ young people
- **gamers with a disability**
- young people engaging in disruptive behaviours in both primary and secondary settings – truancy was also a risk factor in secondary school settings
- young people with behavioural traits like impulsivity, intense or unique interests, a strong need for connection, literal thinking, emotional sensitivity or past trauma.

When does it happen?

Cyberbullying is relational and tends to increase during school terms when students are face-to-face. Reports drop during holidays, especially over summer and term breaks.

The challenges

There are several barriers that can make it difficult to detect and respond to cyberbullying.

- Adults may not understand the platforms young people use, which can lead to underestimating the harm or missing the signs.
- Young people often fear negative consequences if they report, such as losing access to their devices.
- Peers may also dismiss the behaviour as 'just a joke', and anonymity can make it hard to identify who is responsible.

Protective factors

Four broad categories can help inform strategies to help prevent cyberbullying.

1. **Personal resilience** – young people with higher self-esteem and strong emotional regulation are better equipped to cope with online harm and bounce back from negative experiences.
2. **Supportive family environments** – open, non-judgemental conversations and co-created internet rules help young people feel safe, empowered and more likely to seek help when needed.
3. **Positive peer influence** – friends who model respectful behaviour and offer support can reduce the likelihood of cyberbullying and provide a buffer when issues arise.
4. **A 'positive whole school climate'** – when students feel valued and connected, and staff are seen as fair and approachable, they are more likely to report concerns and trust that action will be taken.

Emerging technologies impacting school communities

Artificial intelligence (AI) and sexual extortion

Why child safe AI matters

Children are often overlooked in the design of AI tools. As young people adopt AI rapidly, they face growing risks such as AI-driven cyberbullying, deepfake nudes and sexual extortion.

AI driven cyberbullying

Generative AI is making cyberbullying faster and harder to detect, with tools used to body shame, create deepfake sexual content, and impersonate others using voice cloning. AI can also be used to target someone with abuse, or track and harass them through reverse location searches and doxing (sharing private information without consent).

- 'Nudify' apps use AI to create fake sexualised images. They are easy to access and misuse.
- AI platforms can generate fake or humiliating images, placing individuals in compromising scenarios or altering features to mock or exclude.
- Wearable tech, like smart glasses, can discreetly record and stream content, raising concerns about privacy, consent and cyberbullying.

Sexual extortion

Sexual extortion, sometimes called 'sextortion', is a form of blackmail where someone threatens to share a nude, sexual image or video of someone unless the person gives into their demands.

Tactics may combine deepfakes with hacked personal data to blackmail victims – meaning the victim may not have even shared intimate images.

- Boys and young men are more likely to be targeted for financial sexual extortion by unknown offenders, often linked to overseas criminals.
- Girls and young women are more often targeted for non-financial sexual extortion involving intimate content, usually by someone they know or have met online.

How to support a student who has experienced sexual extortion

- Believe them, tell them it's not their fault and respond with empathy.
- Focus on the current situation, not what could have been done.
- Help them report sexual extortion as well as prevent images being shared (see Reporting to eSafety).

Always follow your school policies and procedures.

Supporting young people

Your role

Develop a positive whole school climate

This is built through consistent, respectful communication across the school. You can:

- **Know your school's values** – be aware of the leadership, parent community and cultural context that shape respectful relationships at your school.
- **Model inclusive language** – use consistent, respectful language when discussing key topics like diversity, discrimination, gender stereotypes, trusted adults and consent.
- **Align with curriculum priorities** – know how your school engages with the Respectful Relationships curriculum and health and physical education program.
- **Support national approaches** – reinforce key messages about respect, personal and social skills, and the impact of gender norms on behaviour and choices.

Engage in respectful relationships education

Respectful relationship education can reduce the likelihood of online harm. In your role:

- **Intervene early** – call out degrading comments, violence or misogyny when you see it.
- **Discuss consent and boundaries** – help students understand respectful behaviour online, especially when content is AI-generated or manipulated.
- **Support reporting** – make sure students know how and where to report sexually explicit deepfake abuse.

Reporting to eSafety

eSafety can help deal with online abuse and harmful online content, including how to report if platforms fail to act:

- **cyberbullying**
  - Sharing **fight videos** online may fall under the definition of **cyberbullying** if they target a child or young person under 18. For more information, visit **Dealing with fight videos**.
- **adult cyber abuse**
- **image-based abuse**
- **illegal and restricted content**

Information and resources

These references provide valuable background on online use and risks and cyberbullying.

- [Digital use and risk: Online platform engagement among children aged 10 to 15](#)

- [What factors protect students from or reduce students' risk of being bullied? Strengthening bullying prevention and response in schools using insights from an analysis of NSW student data 2022-2023](#)

For educators

- [Spotlight on cyberbullying](#) – links to a range of resources across the eSafety websiteand includes downloadable material to help your school community prevent and respond to cyberbullying.

- [Toolkit for schools](#) – over 40 guidance documents to assist school communities to create safer online environments.

- [Best Practice Framework](#) – an evidence- based framework to support the delivery of online safety education.

- [Social media age restrictions hub](#) – to help you understand the social media age restriction changes.

- [ACARA Curriculum Connection: Respectful Relationships](#) – the national curriculum outcomes for developing respectful relationships.

- [The eSafety Guide](#) – information about the latest games, apps and social media, including how to protect personal information and report harmful content.

Professional learning and training

- [Webinars for educators and youth serving professionals](#)
- [Online modules for lower primary educators teaching online safety](#)

News and research for school newsletters

- [Advisories and blogposts](#) – up to date information about emerging issues and technologies.
- [Research](#) – eSafety conducts, evaluates and supports research about online safety for all Australians.

For parents and carers

- [Webinars](#) for parents and carers – live sessions designed to give parents and carers the knowledge, skills and tools to support their children.

- [Online safety for every family](#) (available in multiple languages) – short videos and easy to read advice about how to keep children safe and what to do if something does happen online.

- [Online safety guide for parents and carers](#) (available in multiple languages) – a book about key online safety issues and practical advice about what to do if things go wrong.

- [Parental controls](#) – can be used to support family's online safety when using devices that connect to the internet.

- [Swoosh, Glide and Rule Number 5](#) – an online safety picture book available to watch, download or order as a printed copy.

Find more tailored online safety resources at [esafety/gov.au/parents](#)

For communities

Online safety information

- **First Nations people**
- **LGBTIQ+ community**
- **Culturally and linguistically diverse communities**
- **People with disability**

Easy Read guides

- **Being safe online** – explores the concept of privacy and online friends, and how to get help of something goes wrong.
- **Cyberbullying** – a guide for people under 18 – explains what cyberbullying is, how to report it, and how to get help if you are bullied online
- **What you can do about image-based abuse** – explains image-based abuse and how to get help if it happens.
- **What you can do about abuse through technology** – explains technology- facilitated abuse and how to get help if it happens.

The eSafety website also has tailored online safety information and resources for **Young people**, **Kids**, **Women**, **Seniors**, **First Nations** and **Communities**.

Subscribe and stay up to date

Sign up to eSafety News to stay up to date with new resources, online issues, events, blogs and the latest online safety research.