Key messages

- It is important that young people understand what they post, comment or share online is not confidential.
- Young people should avoid sharing any financial details or personal details into websites unless they are sure they are safe and secure.
- Cyberstalking is when a person is stalked or harassed by another person online. Behaviours can include interacting with every social media post, constant, cryptic and/or intrusive messaging, sexual innuendo, and threats.
- Support is available for people who are being cyberstalked.

Cyberstalking

Cyberstalking is when a person is stalked or harassed by another person online. Stalking behaviours can include interacting with every social media post, constant messaging, that occur in a frequent and intrusive manner, cryptic messages, sexual innuendo, and threats, creation of multiple accounts to bypass blocking or increase the number of messages. The usual goal for all types stalking is to create a sense of fear and the motivation is based on control and intimidation.

Initially, the online perpetrator might appear to be trustworthy because their actions (i.e. requests, online conversation, images, requesting to play games together etc.) are all positive and engaging. However, it is important to remember that it is very easy for people to create false online identities, and this behaviour may escalate into inappropriate requests or messages.

The person committing cyber stalking could be someone they have met online, but it may also be someone they know in real life (for example: a fellow student), and the cyberstalking is an extension of stalking and bullying at school.

Online predators are very clever at using technology to manipulate and deceive. It is important that young people know how to protect their personal information while communicating online.

Actions to protect personal information

- You shouldn't use personal information in usernames or displayed on public profiles.
- Understand that information shared online can be permanent. Information posted and shared on social networking sites may be permanently recorded and users may not have control over who sees or accesses their personal information. Even if a post or information deleted or edited, people may screenshot or be able to review it. This includes teachers, parents and prospective employers. When joining online communities, students are advised to read and understand the privacy policies and settings offered to prevent access to personal information, including images.

- Just as you wouldn't give a person you meet in-person for the first time large amounts of personal or private information, you shouldn't do that to a person online.
- Do not meet in person alone. When establishing a new friendship online, it is very tempting to meet them in person. However, because this friendship is new and communication has only taken place online, it is important that safety is a priority. To ensure safety, it is recommended that the first meeting is arranged to be held in a busy location (e.g. shopping centre) and that the person takes a trusting adult with them.
- Credit card details, bank account details, tax file numbers, passwords or other personal information should never be sent electronically unless on a secure website. This may be indicated by a web address beginning with https:// and a ‘locked’ padlock symbol in the bottom of the screen, which indicates that data is being encrypted.
- If in doubt about the legitimacy of a website, call the organisation it claims to represent. When calling, do not use phone numbers provided on the suspect website or in suspect emails. Use a known phone number or one obtained from a trusted source such as the White or Yellow Pages or a government website. The SCAMwatch website provides further advice on how to identify and report potential scams.
- Encourage students to read user agreements or privacy policies to determine how their personal information may be used in the future. Many organisations use information for marketing purposes and may sell it to other marketing firms. If information is posted on websites that do sell information to marketers, individuals may receive promotional spam emails which can be difficult to stop.

Teaching tips

- Communicating online is part of growing up and maintaining social lives with peers and family. We need to teach students to keep themselves safe.
- Young people want information on the social, psychological and legal consequences of online communication.
- Students respond well to understanding the consequences of the law.
- Inform students that many mobile devices have 'geotagging' activated as an automatic setting. Geotagging can tell users the location of the content of a given picture or other media such as a person’s home address. To disable this go to 'settings', then 'location services'.
- A 'digital reputation' is the opinion that others hold about the user. Students should be encouraged to think about their digital reputation when interacting online. It is important for students and teachers alike to be aware of where their personal data is available on the internet given the potential for it to be permanently accessible by an unknown audience.
- Remind students that just because someone has an 'an established profile' (i.e. has been posting for a long time, and people like/comment on their posts) does not mean they are real. Someone could have made that profile with the sole purpose of cyber stalking someone, and using artificial intelligence to create images and videos of themselves.
- Establishing a cybersafety contact person. This person would provide guidance to students and parents on issues concerning student safety and wellbeing.
- Refer to the Australian Government's esafety website for resources to:
    - educate students and parents about the appropriate use of personal information online, including a reference to information about protecting personal information in the school newsletter
    - integrate teacher resources into the school curriculum to equip students with practical cybersafety skills and knowledge
    - participate in outreach programs to train students, teachers and parents about online safety through the provision of web-based and face-to-face events.

Teacher's responsibility

- Do not investigate, view or email questionable photos. Investigation is the role of the police.
- If possible, isolate the images and turn off the device. Some schools have mobile phone policies that will provide support for this.
- Report the incident to your Principal who will then report to the police. The police consider this a priority 1 and will respond within 24 hours.

Deepfakes and image-based abuse

A deepfake is a photo, video or audio recording that uses artificial intelligence (AI) to create a realistic but false depiction of a real person saying or doing something they did not actually say or do.

While edited images and videos are not new, generative AI tools have made it much easier and faster to create highly realistic content. As a result, deepfakes are becoming more common and accessible.

Deepfakes can be a form of image-based abuse when they depict a person in sexual, explicit or intimate situations without their consent. Although the content is not real, the harm caused is real and significant. Creating, sharing or threatening to share these images can have serious emotional, social and legal consequences.

Sexual deepfakes may be used to:

- harass or humiliate someone
- damage a person's reputation
- exert coercive control in relationships
- distribute content through pornography websites
- create or share child sexual abuse and exploitation material
- provide sexual gratification for others.

Discussing AI, deepfakes and image-based abuse in relationships and sexuality education (RSE) can help students develop the knowledge and skills needed for safe, respectful and responsible online interactions. Key messages may include:

- creating sexual or nude deepfakes of someone without their consent is illegal
- deepfake image-based abuse can cause significant harm
- sharing or forwarding this content is also a form of image-based abuse
- deepfakes can be used to manipulate, threaten or control others in relationships
- students should know how to report image-based abuse and where to access support
- teachers and schools should develop and reinforce strategies to maintain online safety, including privacy surrounding photography and image sharing.

Responding to incidents

The eSafety commissioner has several resources to support responding to and managing deepfake incidents at school:

- Guide to responding to image-based abuse involving AI deepfakes
- Respond | eSafety Commissioner

Relevant resources

Professional development

Outreach programs, Office of the Children's eSafety Commissioner

Outreach programs have been developed to train students, parents and teachers about online safety through the provision of web-based and face-to-face events.

Websites

Staying safe online, Kids Helpline

Office of the eSafety Commissioner

Provides activities, resources and practical advice to help kids, teens, teachers and parents safely enjoy the online world.

Bullying. No Way!

Aims to create learning environments where every student and school community member is safe, supported, respected, valued and free from bullying, violence, harassment and discrimination.

ThinkUKnow for young people 11-17 years old

Informative site for teens on cybersafety. Also has a 'report abuse' tab which is monitored by the Federal Police.

Fact sheets/booklets/videos

Tagged

A video which encourages young people to reflect on the real life consequences of cyberbullying, sexting and a negative digital reputation.

Contacts

Report cyberstalking to Crime Stoppers on 1800 333 000 or visit the Crime Stoppers website. If physical contact is made, contact your local police.

The Federal Police office is located at 619 Murray St, Perth, (08) 9320 3444.

This Background Note relates to the following Learning Activities:

- Safety first
- Respectful relationships online

© 2023 Government of Western Australia Department of Health gdhr.wa.gov.au