

Overview

Cyberstalking is when a person is stalked or harassed by another person using a service of the internet such as email, instant messaging or via a posting in a discussion group. Stalking behaviours can include threats, cryptic messages and sexual innuendo that occur in a frequent and intrusive manner. The usual goal for stalking is to create a sense of fear in the recipient 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, etc.) are all positive and engaging. However, it is important to remember that it is very easy for people to create false online identities. Online predators are very clever at using technology to manipulate and deceive. As a result, it is important that people know how to protect their personal information while communicating online.

Actions to protect personal information

There are strategies that can be implemented to protect our personal information when we are communicating online.

- Only disclose financial information on secure websites.
- 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.

- 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. 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.
- 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.

Teaching tips

- 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.
- 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.

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 Children's 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

Cyberstalking

Background Note

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.

Postscript

This Background Note relates to the following Learning Activities:

- ☐ [Safety first](#)
- ☐ [Respectful relationships online](#)

- ☐ [Why is it important to have good privacy settings on social media?](#)

Date printed

29 March 2024

