Cybersafety: Information for parents and carers

What do I need to be aware of?

This booklet offers advice to support your child in safely navigating their online journey.

Queensland Government

The internet is having an increasing influence on the social development of children. Social media, smart phones and other technologies provide children with wonderful opportunities to learn, be creative and socialise. However, just as with face-to-face interactions, sometimes behaviour between people is inappropriate.

Online content can be posted instantaneously, which creates risks for children when they publish messages without thinking about future ramifications. Once it's online, it can be extremely difficult to remove.

Importantly, just like in the real world, not everyone is a friend. While people can use apps, websites, chat rooms and other online tools to send positive words, compliments and congratulatory messages, others can use the technology to send nasty and inappropriate messages, or pretend to be someone else.

As parents and carers, you play a key role in supporting your child to have a positive and safe online experience. This booklet offers advice and guidance to assist you and your child on their online journey.

Online safety tips

Be proactive

- know which social media apps or websites your child uses and what the age restrictions are. If in doubt, look at The eSafety Guide: *www.esafety.gov.au/key-issues/esafety-guide*
- if you allow your child to have social media, you should also create your own account and add your child as a friend/follower. If your child is under the age of 13, it is important to read *www.esafety.gov.au/parents/skills-advice/are-they-old-enough*
- encourage your child to be open with you about being online. Often, the fear of losing access to social media or their personal devices is why children are hesitant about talking with their parents about online issues

- teach your child how to take a screenshot on their device so they can capture evidence of cyberbullying or inappropriate behaviour
- form clear and agreed rules for your child’s internet use. This may include regular device check-ups where you can review their recent activity
- establish a simple agreement with your child to ensure you all understand the rules and arrangements for use
- remind your child that if they wouldn’t say something out loud or in front of an adult, they should not say it online either.

Responsible interactivity

- ensure that your child knows how to block, unfriend and report inappropriate online behaviour
- know your child’s online friends and followers
- encourage your child to think before they share. They should ask themselves, is it positive, useful and true? What your child says online could affect their friendships, other relationships and prospects for study and work
- review privacy settings regularly as they can change without notification—particularly after device, app or system updates are installed
- introduce a communal charging station where devices are placed at the end of the day to avoid late night use of devices in bedrooms
- enable parental controls from the settings menu on your child’s device to prevent access to specific features and content.

Effective privacy

- help your child to regularly update their privacy settings. Make sure their profile is set to ‘private’ or ‘friends only’
- limit the personal details your child shares online. For example, avoid sharing identifying photos, their full name, date of birth, home address and telephone number. Sharing these can lead to misuse of information by others
- remind your child to carefully consider their choice of profile picture. Using a photo that doesn’t show their face or other personal details is the safest option
- encourage your child to use an online nickname that doesn’t contain their full name or give away personal details
- make sure the updates are downloaded when released to ensure privacy patches or issues identified by the owners of the software are immediately resolved.

Strong passwords

- teach your child how to create a strong password. Passwords should feature a combination of upper and lowercase letters, numbers and symbols
- encourage the use of passwords for online accounts that differ from school, banking or email logins
- reinforce they do not share their passwords with friends or other people and have a routine for updating them.

Location services

Location services can be useful in various ways, including monitoring your child's phone location. There are GPS tracking apps that can be installed for this purpose if desired. However, social media location services can also broadcast your child's physical location to others online.

- consider disabling location services and settings in apps that do not truly require your child's location. In particular, review location services for social media apps and the device's camera. If enabled, photos may contain location information when shared online
- be mindful that whilst many social media sites allow you to share your location, this may also be alerting others that you are away from your home.

Parental controls and filtering

When your child connects their device to the school network, the Department of Education's internet filtering system protects them from malicious web content and inappropriate websites. To help protect your child when they return to your home internet connection, it is recommended you use parental controls and other software tools that allow you to monitor and limit the content your child views or how they interact with others.
Once enabled, parental controls can assist with features such as setting up rules for all connected devices to your home wi-fi, blocking websites and apps, filtering web content, monitoring devices and setting time limits.

Unfortunately, parental controls are not foolproof and do not replace the need for parental supervision. It is important to set clear rules for where your child uses devices within your home, what sites and online activities they can access, and who they are connecting with online.

The Australian Government's eSafety Commissioner offers advice regarding parental controls and other tools to maximise online safety in your home. Check out the parental advice on *Taming the technology: www.esafety.gov.au/parents/skills-advice/taming-technology*.

Google Safe Search

Google's SafeSearch facility is a free feature within the Google search engine. When activated, sites that Google considers inappropriate are filtered from search results. Enabling this feature can remove inappropriate content, such as pornography, from search results: *www.support.google.com/websearch/answer/510*.

Inappropriate online behaviours

Steps to consider if your child is being cyberbullied
Cyberbullying is the use of technology to bully a person and can include a variety of inappropriate behaviours. When children experience cyberbullying, it can be quite distressing and may be difficult for them to talk about. If your child has been cyberbullied, speak with them about what has occurred and remain calm as you listen to their concerns.

You may contact your school if your child is being bullied through school ICT resources, or if inappropriate content has been published by another student at their school.
Help your child capture evidence, report content and unfriend and/or block anyone who makes them feel uncomfortable, harassed or bullied.

Encourage your child to refrain from responding to the bully, this may further inflame the situation.

Promote positive bystander behaviour. Work with your child ahead of time to come up with safe ways to stand up to online abuse they may witness.

Notify the police if physical threats are made or if you have concerns for your child's safety.

Continue to monitor your child's online behaviour. If you have concerns about their wellbeing, counselling and support services are available including Kids Helpline, Headspace, the Office of the eSafety Commissioner and Family and Child Connect.

Report cyberbullying

School devices have a 'report cyberbullying' icon where students can make a complaint with the Australian Government's eSafety Commissioner, find someone to talk to, and get advice on dealing with cyber issues. You may consider bookmarking this webpage on your home devices too.
https://www.esafety.gov.au/report/cyberbullying

Removing and reporting inappropriate content
The fastest and easiest way to remove online content is to ask the person responsible for posting it to remove it. If you don't know who the person responsible is, or if they refuse to delete it, you can report the content to the social media provider for review and possible removal.

Most social media and content-sharing websites will remove content that breaks their terms of service or acceptable-use policies. If you are unsure about the procedure for reporting, there are normally help pages on the site or within the app.

Support pages for common sites:

- Facebook Help Center: facebook.com/help
- Instagram Help Center: help.instagram.com
- Snapchat support: support.snapchat.com
- TikTok Support Center: support.tiktok.com
- YouTube Help: support.google.com/youtube

When is it a legal matter?

If you have concerns for your child's safety, report the incident to your local police. Serious instances of cyberbullying and inappropriate online behaviour may constitute a criminal offence and become a police matter. For example, online content may substantiate the offence of 'using a carriage service to menace, harass or cause offence' (Criminal Code Act 1995 (Cth) s.474.17).

Where students are involved in the taking, distributing or possessing of inappropriate photographs or videos, the content may be considered child exploitation material and these online behaviours may constitute offences against the Queensland Criminal Code. School staff may report incidents of this nature to the police in accordance with departmental procedures.

If you feel that the online content seriously impacts your child's reputation, you may like to seek personal legal advice. Defamatory content may give rise to litigation under the Defamation Act 2005.

How state schools manage online issues and cyberbullying

Bullying and violence are not acceptable at any time. You may report any inappropriate online behaviour to your school principal if it involves bullying between students from the school, or involves the use of school ICT resources.

While some content may be upsetting for you and your child, if the content does not affect the good order and management of a school, it is unlikely that it will constitute grounds for the school to get involved.

If online behaviours or incidents negatively impact the good order and management of your school, your principal can take steps in accordance with their Student Code of Conduct and may:

- apply disciplinary action, such as detention, suspension or exclusion
- report the incident to the police.

Other approaches may include:

- assisting the students responsible to develop more appropriate social skills
- teaching anti-conflict and anti-bullying strategies
- implementing resilience and anti-bullying programs
- conducting mediation sessions
- addressing bullying and cyberbullying in the curriculum.

Generally, for privacy reasons, a school cannot provide personal details of other students involved in an incident or details of any actions being taken towards them. However, schools can generally advise whether a complaint has been investigated and substantiated, and whether disciplinary consequences have been given.

Key links for cybersafety information

Department of Education Cybersafety website:
qld.gov.au/cybersafety

Cybersafety Facebook page:
facebook.com/QEDCybersafetyAdvice

Organisations and initiatives

Office of the eSafety Commissioner:
esafety.gov.au

Report cyberbullying:
esafety.gov.au/report/cyberbullying

Kids Helpline:
kidshelpline.com.au/parents

Headspace:
headspace.org.au

Family and Child Connect:
familychildconnect.org.au

Think U Know, Australian Federal Police:
thinkuknow.org.au