

An illustration of a hand with a blue sleeve pointing at a tablet screen. The screen displays the title. To the right of the hand is a red shield with a white cross. The background is a vibrant green with geometric patterns, white clouds, and small white stars.

Online awareness: **A guide** for parents and caregivers

Positive and responsible technology use

As a parent or caregiver, you have a right to know what your children are doing online. This guide offers steps to support your child to have a positive and safer online experience within your home.

DRAFT

FOR CONSULTATION

More and more, the internet is playing an important role in the social development of children, helping them learn how to interact with each other. Social media, smart phones and other technology provide children with wonderful opportunities to learn, be creative and socialise. However, bullying and harassment can occur anywhere children gather, including when they are online.

Being online is more often than not a positive and fulfilling experience for children, although it can be challenging. Content can be posted instantaneously, but the downfall is that children can potentially post messages without thinking about the future ramifications. Once it's online, it could be there forever.

Importantly, just like in the real world, not everyone is a friend. People can use apps, websites, chat rooms and other online tools to send nasty and inappropriate messages to each other.



Social media tips

- Know which social media (apps or websites) your child uses.
- Create your own social media accounts and add your child as a friend/follower or know your child's social media passwords so you can access their accounts.



Strong passwords

- Ask your child if they know how to create a strong password. They should feature upper and lower case letters, numbers and symbols.
- Encourage them to use passwords for online accounts that differ from their school login.
- Make sure they keep their passwords to themselves and you.



Effective privacy

- Ask your child to regularly update their privacy settings. Make sure their profile is private and only accessible by people they know.
- Limit the personal details your child shares on online accounts. For example, remove identifying photos, full name, date of birth, home address and telephone numbers.
- Ask your child to use a cartoon avatar for their profile picture or share a photo that doesn't show their face.
- Encourage them to use an online nickname that doesn't contain their full name or give away too much personal detail.

Responsible interactivity

- Know your child's online friends and followers. Make sure your child understands they shouldn't become friends or communicate with anyone online unless they know and trust them in the real world.
- Encourage your child to think before they share. They should ask themselves, is it true, useful and positive? The things your child says online could affect their friendships, other relationships and prospects for study and work.



- Make sure your child knows how to block, unfriend and report inappropriate online behaviour.

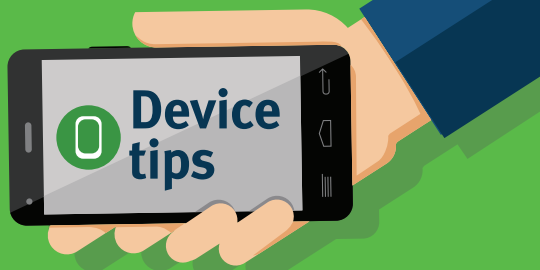
Location services/ settings

Most technology features have positive and negatives. Location services are a good example of this. On one hand, location services can be a useful way to monitor your child's phone location – there are GPS tracking apps that can be installed for this purpose if desired. But, social media location services can broadcast your child's physical location to the world.

- Disable the location services/settings in every social media app used by your child.
- Disable location services for their device's camera as well.



- Monitor privacy settings; they can change without notification and after installing device, app and system updates.
- 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 to prevent access to specific features and content.



Be proactive!

- Encourage your child to be open with you about being online. Often, the fear of losing access to social media is why children are hesitant about talking with their parents about online issues.
- Take a proactive approach and establish clear and agreed rules for your child's internet use. This may include, at any given moment, your child is required to hand you the device for you to view.

- Teach your child how to take a screen shot on their device, so they can capture evidence of cyberbullying.
- Promote positive bystander behaviour. Work with your child ahead of time to come up with safe ways to stand up to any online abuse they may witness.

- Encourage your child to never bully back.
- If your child thinks they are being bullied, or encounters offensive online content, encourage them to find someone they feel safe talking to, such as yourself, a relative, a teacher or a trusted adult.

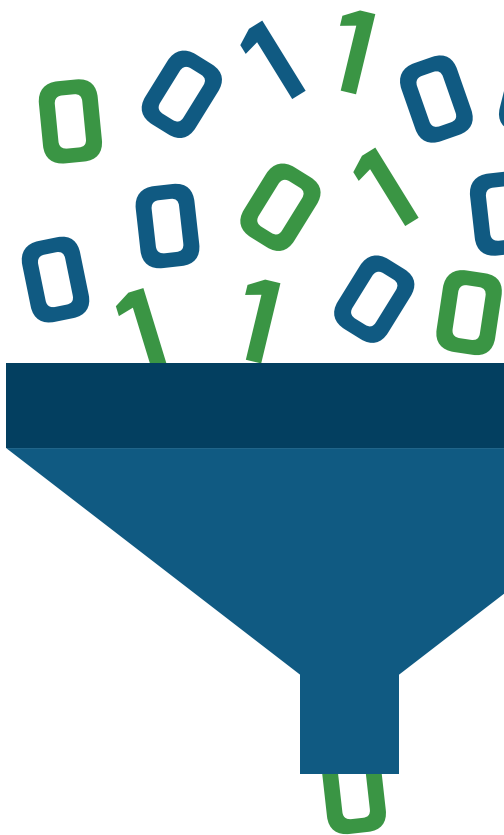
Responsible adults can help your child ignore, report and block the other person.



Internet filtering tools in your home

When your child connects their device to the school network, the department's web 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 install some level of internet filtering.

Unfortunately, filtering and monitoring systems are not fool-proof and do not replace the need for parental supervision when children are online. 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.



Cybersafety help button

Consider installing the Cybersafety Help Button on all of your family's devices. This is a free application that gives children the ability to report cybersafety concerns online. It also gives them access to help, resources and information 24 hours a day. It's available on all state school computers.

www.communications.gov.au/online_safety_and_security/cybersafetyhelpbutton_download

Google SafeSearch

Google's SafeSearch facility is a free feature within the Google search engine. When it is activated within an internet browser, sites that Google considers inappropriate are filtered from search results. Enabling this feature can remove inappropriate content, such as pornography, from search results.

<https://support.google.com/websearch/answer/510>

Home internet filtering

There are many products that offer free and paid web filtering. While some may only cover a single device, others may cover many devices within the one home internet service. Products such as Microsoft Family Safety, Norton Online Family, Bluecoat K9,

OpenDNS Home internet security, Mobicip and Net Nanny offer web filtering. Research the product that suits your family's needs. A recent European study evaluated some of these products, so consider reading it for more advice.

www.sipbench.eu



Removing and reporting inappropriate content

The fastest and easiest way to remove online content is to ask the person responsible 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 administrators 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 these sites or within these apps.

Safety reporting links for some common sites:



Facebook Family Safety Center – facebook.com/safety



Instagram Help Center – help.instagram.com



Snapchat support – support.snapchat.com



YouTube Help Center – support.google.com/youtube

What should you do if your child finds inappropriate content about them?

Bullying and other inappropriate online behaviour can be distressing and may be difficult for children to talk about.

Therefore it's important to 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.

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



How state schools manage online issues and cyberbullying

Bullying and violence are not acceptable at any time. You should 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.

Know that while some online 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 a school to get involved.

However, if online behaviours negatively impact the good order and management of your school, your principal can take steps under their Responsible Behaviour Plan for Students or Code of School Behaviour.

Also, the department's Safe, Supportive and Disciplined School Environment procedure covers the provision of a safe and supportive learning environment, including the online learning environment.

Behaviour management documents provide guidelines on acceptable online behaviour in school. They include the Code of School Behaviour and ICT Acceptable Use Agreement.

If an online incident impacts on the good order and management of your school, the principal may:

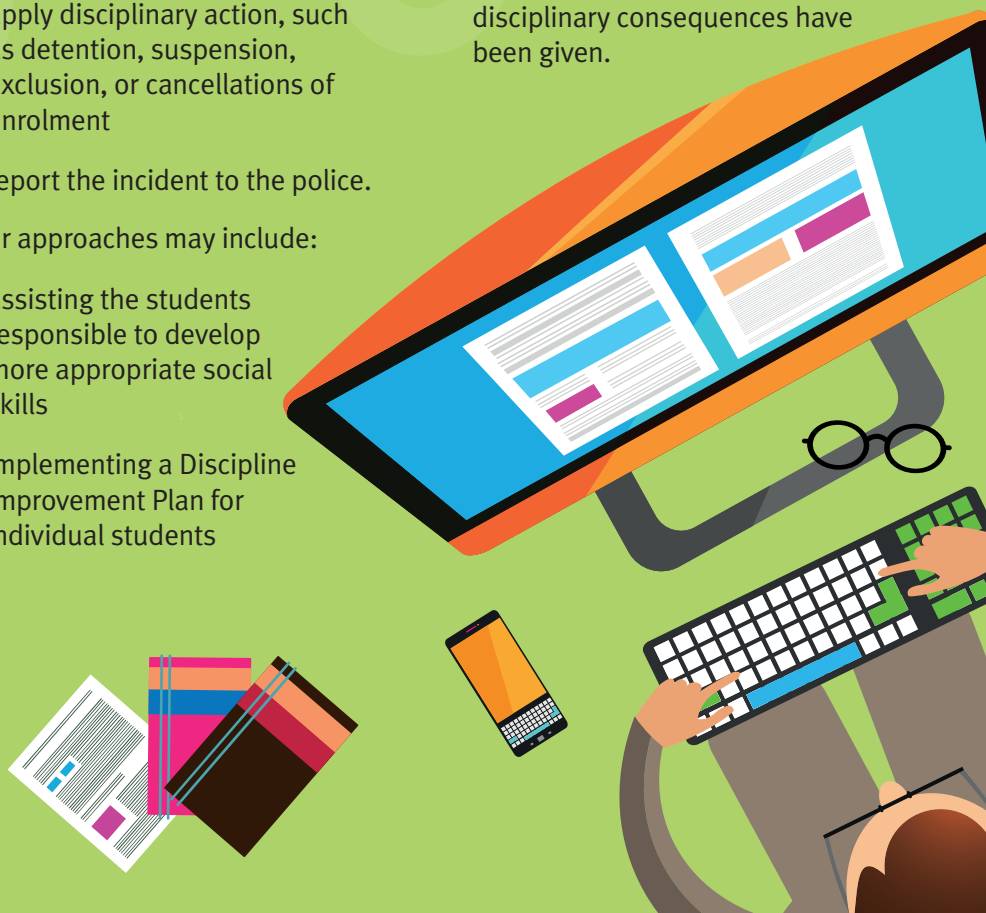
- apply disciplinary action, such as detention, suspension, exclusion, or cancellations of enrolment
- report the incident to the police.


Other approaches may include:

- assisting the students responsible to develop more appropriate social skills
- implementing a Discipline Improvement Plan for individual students

- 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.





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, 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 online content may give rise to litigation under the Defamation Act 2005.

Further information

Department of Education and Training

Incident management:
CyberSafety.ReputationManagement@dete.qld.gov.au

Cybersafety website:
qld.gov.au/cybersafety

Organisations and initiatives

Bullying. No Way! Australian Government:
bullyingnoway.gov.au

Office of the Children's eSafety Commissioner:
esafety.gov.au

Cybersafety Help Button
esafety.gov.au/complaints-and-reporting/cybersafety-help-button

Kids Helpline:
kidshelp.com.au/grownups

Meet the Creeps – Creep Quiz: Are you safe online? Queensland Government:
creepquiz.eq.edu.au

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

Online safety awareness: A guide for parents and caregivers

