PROFILES

Use a nickname and a profile picture that doesn't show your face.

5 'P's for a positive digital footprint

POSITIVE

Make sure online information about you is as positive as possible.

5 'Ps' for a positive digital footprint

PERMISSION

Make sure you have a grown-up's permission to use a new site or app.

5

for a positive
digital footprint

PROTECT

Keep evidence and never bully back, tell someone!

5 for a positive digital footprint

PRIVACY

Keep your passwords and personal details secure

5 'Ps for a positive digital footprint

Department of Education, Training and Employment

Cybersafety and cyberbullying

A guide for parents and caregivers

Queensland Government

Contents

What is cybersafety?	4
Why is cyberbullying an issue?	5
Where does cyberbullying occur?	5
How can I promote my child's cybersafety?	6
What should I do if my child is cyberbullied or receives inappropriate content online?	7
What if my child is responsible for inappropriate online behaviour?	7
How can I remove inappropriate content?	8
How do I report an incident to a website operator?	8
How do state schools manage cybersafety issues and cyberbullying?	9
When is it a police matter?	10
What web filtering and parental control software is available?	10
Further information	11

Cybersafety and cyberbullying

The internet, mobile phones and instant messaging provide wonderful opportunities for children to learn, be creative and socialise online. They also provide opportunities for inappropriate behaviour, bullying and harassment to occur — causing pain and suffering to the targets of such behaviour.

This guide provides important information for parents about cybersafety and cyberbullying. It suggests what you could do if your child is the target or is responsible for inappropriate online behaviour.

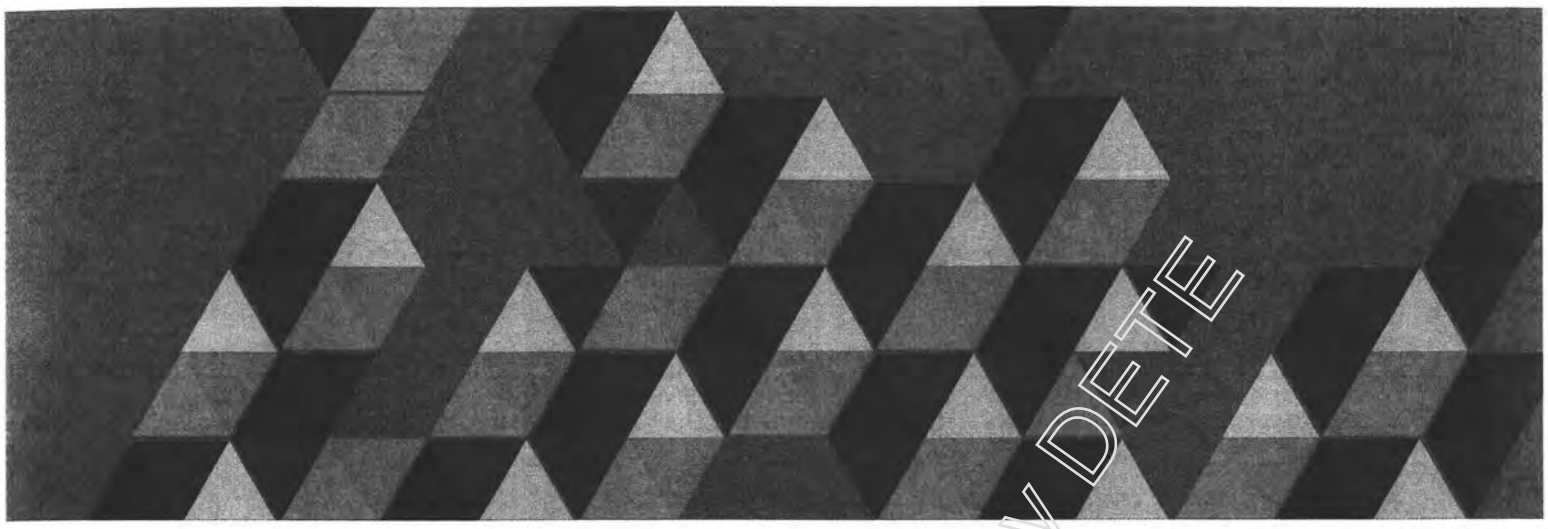
What is cybersafety?

Cybersafety is a broad term referring to appropriate and responsible behaviour online — it covers online privacy and information protection, good manners and behaviour online, and knowing how to get help to deal with online issues.

Cyberbullying is when technology, such as email, mobile phones, chat rooms and social networking sites, are used to verbally or socially bully another person. Bullying is an ongoing abuse of power to threaten or harm another person.

The following are some common examples of cybersafety issues, including cyberbullying:

- sending or posting abusive, threatening, humiliating or harassing messages via text, social networking sites or email
- forwarding others' personal emails, messages, pictures or videos without their permission
- uploading embarrassing or degrading images or videos involving other children (including fight videos)
- taking and sending sexually explicit images of other children using mobile phone or web applications
- using social networking sites or blogs to post inappropriate photographs or messages about other children or school staff
- excluding children online through emails, chat and social networking sites
- imitating others or assuming a child's identity, then sending and posting material which damages their social status or relationships with others
- making prank calls to another child's mobile phone.



Why is cyberbullying an issue?

The internet is playing an increasingly important role in the social development of children. It is providing more and more opportunities for them to engage with other children and adults and get instant feedback. It is therefore not surprising that children may also use this technology as a way to harass and intimidate others.

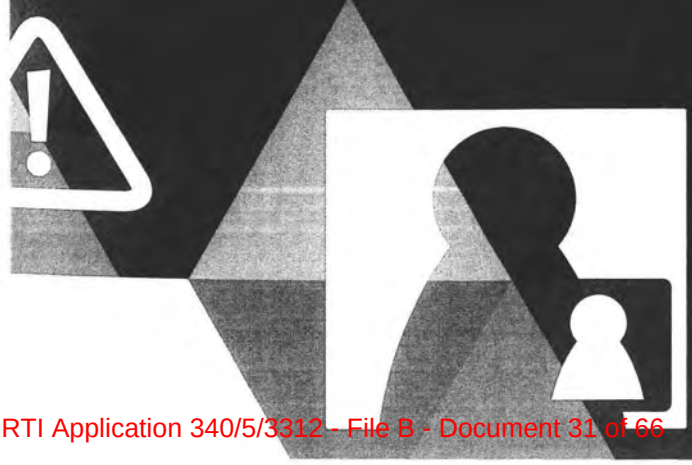
The internet allows information to be sent to a large audience instantly. It also provides a sense of anonymity. With an ability to send material to others under a false name or details, children can easily post negative or harmful comments without fear of being caught.

Compared with face-to-face interactions, the internet also gives people the opportunity to plan what they want to say for maximum impact on others. This allows those who cyberbully to inflict severe emotional and psychological trauma on other children.

Where does cyberbullying occur?

Cyberbullying can take place anywhere that children have access to technology. Some of the most common places include:

- **social network websites and apps such as Facebook and Twitter**
- **media sharing platforms such as YouTube, Instagram and Tumblr**
- **instant messaging applications such as Skype or Facebook Chat**
- **mobile phone data use and SMS and**
- **online gaming.**



How can I promote my child's cybersafety?

Parents can use a number of simple strategies to enhance cybersafety, such as:

- place computers in spaces which are visible and open, like a family room
- monitor or supervise your child on the internet and conduct some "shoulder surfing" or "spontaneous" observing when your child is online. Be aware of what your child is doing on the internet and display an interest in their cyberspace knowledge and experience
- discuss a plan with your child to address cybersafety and cyberbullying. Ensure they know you will be supportive if they report something to you
- reassure your child they will not lose access to their technology if they report anything to you. Many children see this as punishment
- review the age suitability of any social networking sites your child joins
- review your child's contacts, followers and page content on social networking sites/apps to help you manage their safety and reduce the risk of them associating with inappropriate contacts and content
- educate yourself on the latest threats facing children online
- try to keep communication with your child open and positive so they trust you viewing their profile
- create an account on the social networking site/app your child is using and request to become friends or follow their account. Even if your child resists your request it can still be positive for you to have your own account on the social networking site/app. This can increase your familiarity and understanding of the online environments your child is using
- reinforce the need to keep passwords private and updated regularly, but consider having access to your child's password yourself
- ensure your child understands the implications of posting images and other content on the internet
- educate your child about appropriate online behaviours. Take time to sit with your child and participate together on the internet. Assist in developing the knowledge they need to communicate responsibly and respectfully with friends, family and other internet users
- set clear rules about your child's mobile phone and online activities. Talk with your child about which websites and internet activities they are allowed to access
- consider installing appropriate software which has the ability to limit internet usage times and monitor/restrict website activity
- consider installing on your computer the 'cybersafety help button', available from the Commonwealth Department of Broadband, Communications and the Digital Economy's website: www.dbcde.gov.au/online_safety_and_security/cybersafetyhelpbutton_download
- ensure you are aware of the software and app features installed on your child's mobile phone, music or tablet device. Many apps have age suitability recommendations and require age confirmation prior to downloading/use. Additionally, many devices support parental controls which prevent access to specific features or content. These controls can be enabled in the settings menu on your child's device. Consult the device documentation for further information.

What should I do if my child is cyberbullied or receives inappropriate content online?

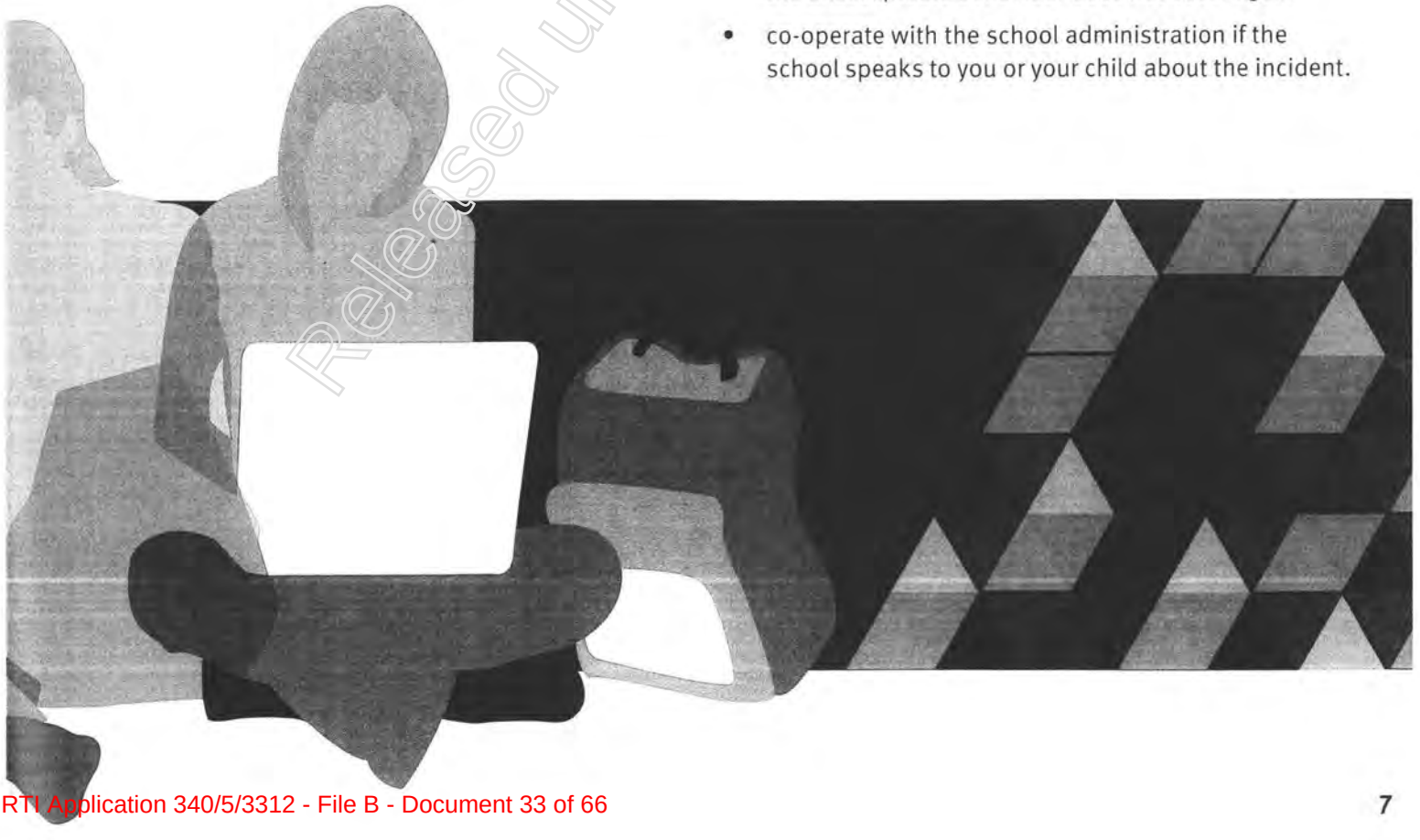
Cyberbullying and other cybersafety incidents can be distressing and may be difficult for children to talk about with their parents. Therefore it's important for parents to keep in mind to:

- encourage your child to maintain social connections with friends and family; this may help if your child's self-esteem has been affected by the incidents
- notify the police if physical threats are made, your child receives inappropriate content or you have concerns for your child's safety generally
- ask the mobile service provider or website operator to investigate and remove the inappropriate material
- help your child block anyone who makes them feel uncomfortable, harassed or bullied
- not respond on your child's behalf — this may further inflame the situation.

What if my child is responsible for inappropriate online behaviour?

If you find your child is involved in inappropriate online behaviour or cyberbullying:

- explain how the behaviour may have caused harm to the other person, even though it happened in cyberspace
- explain that their behaviour has been unacceptable
- if the behaviour is serious, you may consider removing the child's access to technology devices for a period of time, or installing software to restrict their internet/mobile phone activities
- carefully monitor your child's technology use to ensure the unacceptable behaviour does not occur again
- co-operate with the school administration if the school speaks to you or your child about the incident.



How can I remove inappropriate content?

The quickest and easiest way to remove online content may be to ask the person(s) responsible to remove it.

If you don't know who the responsible person(s) is, or if they refuse to delete the inappropriate or offensive content, you could contact the relevant internet or mobile service provider or website operators.

Most website operators will remove content that contravenes their terms of service and/or acceptable use policies. When making a report, read the service provider/host terms and conditions and advise them how the content breaches those conditions.

How can I report and have it removed?

Social networking sites

Most social networking providers have a "Report/Block this Person" or "Report Abuse" link on their pages or on the user's profile. You or your child can report the content and ask to have it removed. These are also often available in mobile applications.

Safety reporting links for some common sites

Facebook:
www.facebook.com/safety

Instagram:
www.help.instagram.com/15447597469/?ref

YouTube:
www.youtube.com/t/contact_us

Twitter:
www.support.twitter.com

Tumblr:
www.tumblr.com/help

Moshi Monsters:
www.moshimonsters.com/parents

Club Penguin:
www.clubpenguin.com/parents

Instant messaging

For chat applications, click on the 'Help' tab and select the report abuse option.

Mobile phones

Most mobile service providers will accept complaints and requests to have content removed when made by the account holder.

Mobile phone network provider contacts

Telstra	1800 805 996
Optus	1800 780 219
Virgin Mobile	1300 555 100
Vodafone	1800 638 638

How do Queensland state schools manage cybersafety issues and cyberbullying?

Cyberbullying and other cybersafety issues may affect the good order and management of the school where it involves:

- bullying between children who attend the school
- images or videos of children on the school premises
- a student at the school possessing or distributing offensive video, images or texts while at school
- school information and communication technologies (ICT) resources being used.

The above are examples only — there may be other incidences that affect the good order and management of the school.

The *Safe Supportive and Disciplined School Environment* procedure covers the provision of a safe and supportive learning environment, which can include cyberspace as it relates to the school and students. Schools have behaviour management documents in place such as the *Responsible Behaviour Plan for Students* or acceptable use agreements. These documents provide guidelines on acceptable online behaviour in a school context.

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

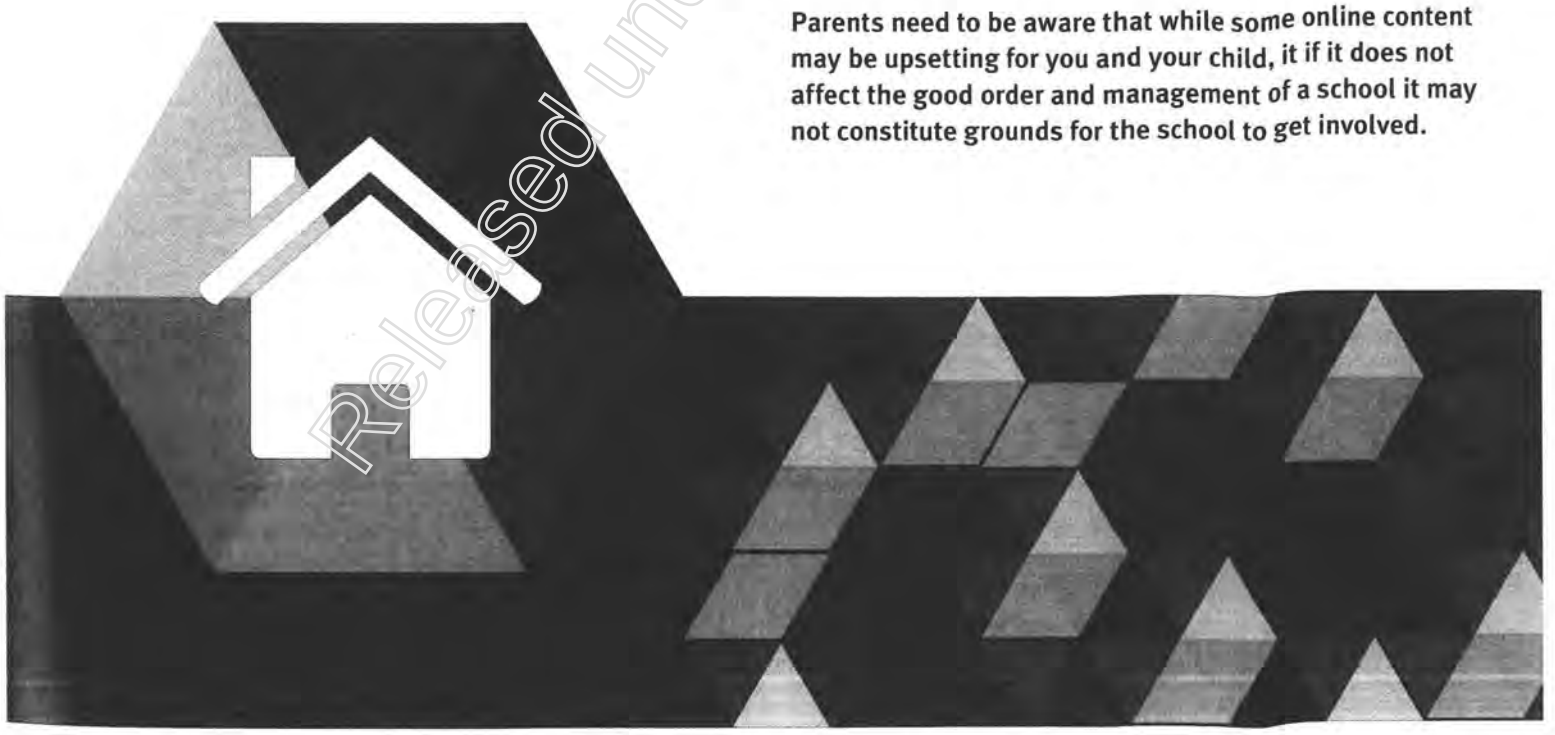
- apply disciplinary action, including suspension and/or exclusion
- report the incident to the police.

Other approaches may include:

- assisting the student(s) responsible to develop more appropriate social skills
- implementing a behaviour management plan for individual students
- teaching about conflict and bullying
- implementing resilience and anti-bullying programs
- conducting mediation sessions
- addressing bullying and cyberbullying in their curriculum.

Generally, for privacy reasons, a school cannot provide the personal details of other students involved in an incident or any actions being taken towards them. However schools can advise that a complaint has, or has not, been investigated, whether or not it has been substantiated and whether or not the school has decided to take disciplinary action without being specific.

Parents need to be aware that while some online content may be upsetting for you and your child, it if it does not affect the good order and management of a school it may not constitute grounds for the school to get involved.



When is it a police matter?

If you have concerns for your child's safety you may report the incident to the Queensland Police Service. Serious instances of cyberbullying and online content/behaviour may constitute a criminal offence.

The key relevant Commonwealth law is 'Using a carriage service to menace, harass or cause offence' *(Criminal Code Act 1995 (Cth))*.

Queensland laws that may also apply include (Criminal Code):

- unlawful stalking
- possessing, distributing and making child exploitation material.

Where the content in question involves a Queensland state school, staff may report the matter to the police in accordance with departmental procedures.

What web filtering and parental control software is available?

For information on web filtering and parental control setup refer to the following government and industry websites:

Queensland Department of Education, Training and Employment
www.education.qld.gov.au/smartclassrooms/mis/filtering.html

Australian Internet Industry Association
www.iia.net.au

Stay Smart Online
www.staysmartonline.gov.au

Students issued with departmental laptops have a web filtering system installed on the device which operates when connected to a school, home or other network.