Parent’s guide to online safety

Practical, issue-focussed information and advice for parents of children of all ages.
With the aim to help guide children and young people toward safe, enjoyable experiences online, the Office of the Children's eSafety Commissioner (the Office) hopes to encourage behavioural change—where Australian children and young people act responsibly online—just as they would offline.

To achieve this, we hope to both educate and help prevent harmful online behaviour from occurring in the first place. As parents, you know your child better than anyone, and have the best opportunity to help educate them so they can explore, safely.
Cyberbullying is the use of technology to bully a person or group with the intent to hurt them socially, psychologically or even physically.

As a parent, you can help your child and encourage them to take control of the issue. Talk to them about cyberbullying before it happens. Together you should work out strategies to address any potential issues and reassure your child that you will be there to support them.

Cyberbullying behaviour may include:
* abusive texts and emails
* hurtful messages, images or videos
* imitating others online
* excluding others online
* humiliating others online
* nasty online gossip and chat.

By reporting it, talking about it and supporting each other, we can stop it.

For many children and teenagers, their online life is an important part of their social identity. They can’t just ‘switch it off’. Many young people do not report cyberbullying to their parents as they fear that they might lose access to their devices and the internet.

Young people may also be concerned that parents’ actions will make cyberbullying issues worse, so it is important for you to remain calm and supportive.

Trolling

Trolling is when a user intentionally causes distress by posting inflammatory comments online.

Trolling differs from cyberbullying in that trolls aim to gain attention and power through disruption of conversation by encouraging a defensive reaction from those they attack. Cyberbullying usually focuses less on the reaction of the victim, and more on the feelings and authority of the bully. Cyberbullying is usually repeated behaviour, while trolling can be one-off.

What can I do?

As a parent, you can help your child and encourage them to take control of the issue. Talk to them about cyberbullying before it happens. Together you should work out strategies to address any potential issues and reassure your child that you will be there to support them.

+ Report the cyberbullying material to the social media service where it happened.

Social media services should remove cyberbullying material that has been reported and is in breach of their terms and conditions. Most social media services have a reporting area on their website. The Office website also provides information about how to report material on various services.

+ Collect details of the cyberbullying material. You might need to do this before you report it to the site. A simple way to collect this information is by taking a photo or screenshot or copying the URL.

If you submit a complaint to the Office about cyberbullying material, you need to provide this information.

+ Report cyberbullying to the Office of the Children’s eSafety Commissioner.

+ Block the person. We recommend that you help your child block or unfriend the person upsetting them, so they cannot continue to upset them while the material is being removed.

++ Remember that if your child has been involved in cyberbullying, and seems distressed or shows changes in behaviour or mood, it may be advisable to seek professional support through Kids Helpline.

Kids Helpline is a free and confidential online and phone counselling service for young people, available 24 hours a day, 7 days a week on 1800 55 1800.

Cyberbullying behaviour may include:
* abusive texts and emails
* hurtful messages, images or videos
* imitating others online
* excluding others online
* humiliating others online
* nasty online gossip and chat.

Trolling

Trolling is when a user intentionally causes distress by posting inflammatory comments online.

Trolling differs from cyberbullying in that trolls aim to gain attention and power through disruption of conversation by encouraging a defensive reaction from those they attack. Cyberbullying usually focuses less on the reaction of the victim, and more on the feelings and authority of the bully. Cyberbullying is usually repeated behaviour, while trolling can be one-off.

What can I do?

As a parent, you can help your child and encourage them to take control of the issue. Talk to them about cyberbullying before it happens. Together you should work out strategies to address any potential issues and reassure your child that you will be there to support them.

+ Report the cyberbullying material to the social media service where it happened.

Social media services should remove cyberbullying material that has been reported and is in breach of their terms and conditions. Most social media services have a reporting area on their website. The Office website also provides information about how to report material on various services.

+ Collect details of the cyberbullying material. You might need to do this before you report it to the site. A simple way to collect this information is by taking a photo or screenshot or copying the URL.

If you submit a complaint to the Office about cyberbullying material, you need to provide this information.

+ Report cyberbullying to the Office of the Children’s eSafety Commissioner.

+ Block the person. We recommend that you help your child block or unfriend the person upsetting them, so they cannot continue to upset them while the material is being removed.

++ Remember that if your child has been involved in cyberbullying, and seems distressed or shows changes in behaviour or mood, it may be advisable to seek professional support through Kids Helpline.

Kids Helpline is a free and confidential online and phone counselling service for young people, available 24 hours a day, 7 days a week on 1800 55 1800.
Chat and social networking are great ways to stay in touch and find new friends.

Social networking describes a variety of services like Facebook, YouTube, Snapchat, Instagram, World of Warcraft, Moshi Monsters, Twitter, Skype, Minecraft and many others. All of these services enable direct interaction between individuals. Users can post information about themselves, display photos, tell people what they’ve been up to, chat and play games. Social networking forms a part of the social identity of many young people.

There are some risks though, including sharing with people they do not know or trust, not being able to control where a photo or video has been shared, or meeting people in real life who they only otherwise know online.

As a parent, you can help your child have positive experiences on social networking sites.

Stay involved in your child’s use of technology. Set up your own account and learn about privacy settings so you can understand how you can best protect your child. It can be fun for you too!

Read the ‘terms of use’ on social media services and make sure your child understands what is expected. Some sites, like Club Penguin, are created especially for children. Many, such as Facebook and Instagram, require users to be at least 13 years of age (often to comply with US laws about the collection of children’s personal data). It’s also helpful to check the age ratings set by app stores too before downloading an app—bearing in mind that these age ratings can sometimes differ from those for websites of the same service.

Advise children to set their accounts to private so that the only people who can view their information are those they trust.

Encourage children to think before they put anything online and to be respectful of others. Information posted online can be difficult or impossible to remove. An inappropriate image posted today may have a long term impact on their digital reputation.

Show your child how to manage location services on their phone so they are not inadvertently broadcasting their location. Help them to set up alerts to let them know if they have been ‘tagged’ in photos that have been posted by others.

Remind children to be careful when making new friends online; people may not be who they say they are. They should never arrange to meet an online friend unless a trusted adult is with them.

Report any cyberbullying or inappropriate content to the social networking site and show children how to do this too. If the social media service fails to remove the material, you can make a complaint to the Office of the Children’s eSafety Commissioner.
Unwanted contact

Online, children can communicate with people they don’t know or have not met in real life.

While being in contact with new people can be exciting, the anonymity offered by the internet can allow these new contacts to cover their true identities.

For example, someone who says they are a 10-year-old girl could actually be a 40-year-old man. This anonymity means that sexual solicitation and online grooming can occur online and are serious risks.

Online grooming and the procuring of children over the internet is the illegal act of an adult making online contact with a child under the age of 16 with the intention of facilitating a sexual relationship. Sexual solicitation is where someone is asked to engage in a sexual conversation or activity—or to send a sexually explicit image or information.

More information is available from the Australian Federal Police (AFP). The AFP investigates suspected cases of online grooming.

What can I do?

+ Encourage your children to tell you or another trusted adult if there is a threat to their safety. You can also contact the police.
+ Help your child report and block the contact or remove them from your child’s friends list.
+ Encourage your child to change their profile settings so that their personal details are kept private.
+ Keep evidence. This can be useful in tracking the person posting unsuitable material.
+ Reassure your child that you will always support them and not block their internet access if they report that they are uncomfortable or worried about what has been said online.
+ Be alert to changes in your child’s behaviour or mood that are concerning, including increased or decreased sexualised behaviours and/or apparent confidence, clinginess or withdrawal, anxiety or sadness and changed interactions with friends. Explore your concerns with them and, if necessary, seek professional help.

++ Reports can be made directly to the AFP about abuse or illegal activity online using the online child sex exploitation form. Parents can also click on the Report Abuse button on the ThinkuKnow or Virtual Global Taskforce websites.

If you believe a child is in immediate danger, call Triple Zero (000), Crimestoppers on 1800 333 000 or your local police station.

esafety.gov.au/unwantedcontact
It’s important to discuss the consequences of sexting with your children. If their image has been viewed by others they may be publicly bullied and have sexually inappropriate comments made about them by friends and strangers, including adults.

Talk to your children about the potential social, academic, employment and legal implications of posting inappropriate material of themselves or others online.

If sexting has already negatively affected your child, help them to identify where the images might be. Send take-down requests to all sites as well as to all other children and send messages to all other children who may have received an image and ask them to delete it immediately.

Remind your child to delete any sexual content they receive from others and avoid forwarding this type of content.

Remind your child to consider the feelings of others when taking photos and distributing any content by mobile phone or online.

Seek professional support if you are worried that your child is vulnerable.

If you are concerned that a sexting incident may be a criminal matter, contact your local police.

If your child has been involved in sexting, remember to stay calm and be reasonable about the consequences. Sexting is not uncommon behaviour and your child is not alone in being negatively impacted. Rather than adding to the distress, focus on finding a solution for your child.
To many parents it seems as though children and young people are constantly online.

Too much time online

Often they seem to be engaged in more than one task at a time; for example, downloading and listening to music while studying and chatting with friends or sending messages on their mobile phones.

The number of hours that children and young people spend online can vary significantly. There is no guideline for the ‘right’ amount of time for children to spend online, however, if their online activity appears to impact negatively on their behaviour or wellbeing, or that of the family, it may be time to discuss expectations and establish time limits.

It’s important to remember that some of the time your children spend online may be related to their education.

What can I do?

+ The longer you wait to address the issue, the more difficult it can be to overcome. So if you see an emerging problem arising from excessive use, act on it right away.

+ Talk to your child about the concerns you have and monitor what games, apps and devices are bought or used by your child.

+ You may like to install a program on the device your child is using which can be adjusted to limit the amount of time an internet connection will be available on that device.

+ Consider implementing family agreements about the amount of time your children can spend online. A similar approach can be used to limit access to devices.

+++ If your child seems particularly anxious or irritable, or you notice them seeming isolated from friends or other activities, there may be an underlying mental health issue. Talk to your child’s school or your GP if your concerns extend beyond screen time.
Inappropriate, offensive & illegal content

Inappropriate, offensive or illegal content may include topics, images or other information that are prohibited in Australia or could be damaging to young people online.

Children and young people may not deliberately seek out inappropriate content. They may inadvertently access content while undertaking online searches, they may seek it out, or be referred to it by others.

Young people with smartphones might also be able to discover content that may be blocked by home and school internet filters.

Offensive or illegal content may include topics, images or other information that are prohibited in Australia or could be damaging to young people online. Offensive or illegal content can expose children to concepts that they are not ready to manage and that may breach social and cultural norms.

Some content can be distressing for children. They may not report it to parents or teachers as they may be ashamed of what they have seen, particularly if they sought it out.

This is content that may:
+ Include footage of real or simulated violence, criminal activity or accidents, promote extreme political or religious views or be sexually explicit. This can include illegal images of child sexual abuse.
+ Promote hate towards individuals or groups on the basis of race, religion, sexual preference or other social/cultural factors, instruct or promote crime, violence or unsafe behaviour, like bomb or weapon making, anorexia, drug use, gaining unauthorised access to computers, fraud or terrorism.

What can I do?
+ Encourage your child to tell you about inappropriate content they have come across and make a complaint about specific content.
+ Limit their exposure to inappropriate content by supervising their online time where possible.
+ Install filters, labels and safe zones that enable you to reduce their risk of exposure to unsuitable or illegal sites.
+ Keep them connected to trusted friends and family online and offline.
+ Help your child use search engines to locate websites. Consider developing a list of favourites for younger children.
+ Reassure your child that access to the internet will not be denied if they tell you about seeing inappropriate content.
+ If you are worried, or your child is vulnerable, please seek professional support.
+ Report inappropriate content to the site administrator.
++ The Office can investigate complaints about content that may be illegal or prohibited. Report this content to esafety.gov.au/reportillegalcontent
Safeguards

If a child has access to an internet-enabled device, they also have access to an extensive amount of content across the web.

There are many ways parents can help their children to explore safely.

What can I do?

+ Put in place online safeguards and parental controls—settings, filters and products that help block certain content so that you are better able to protect what your children see online. Parental controls are available for most devices in the form of pre-installed settings that you can activate, or via the installation of free or commercial software.

Some examples are:

+ Customisable computer accounts set up for your children.
+ Settings that you can apply to your computer to restrict access to downloads, apps, purchasing, games and to set internet usage time limits.
+ Settings you can apply to your router to restrict access to online content.
+ Apps or settings applied to your child’s mobile phone to restrict access to browsers, apps, social networking sites, inappropriate content, photo and/or video sharing sites, streaming, and gaming.
+ Commercial or free internet filters which can alert you to contact from strangers outside of approved social networks, restrict access to inappropriate content, monitor your child’s online activity, restrict online usage times, and track GPS location, calls, SMS and contacts.
+ Remember that no single parental control tool is 100 per cent effective. Some content and sites can be encrypted in such a way that they are not recognised by parental controls, or a tech-savvy child may have the ability to bypass parental controls.

You can also:

+ Encourage and model good behaviours with your kids around their use of connected devices, for example not bringing devices to the dinner table.
+ Set healthy limits about how much time is spent online each day, and for what purpose.
+ Implement boundaries such as only using devices in a ‘safe space’, like the living room, or having an open door policy when children use devices or computers in the bedroom. Be prepared to stick to these boundaries yourself.
+ Learn to understand the devices your children use, and talk to them about the importance of staying safe online and being aware of the behaviours of themselves and others.
+ Establish and maintain trust. It’s hard to monitor your children’s online activity at all times so trust is important.

Further information about discussing these issues with your children can be found at: esafety.gov.au/chatterbox
Help and resources

Online counselling
If you suspect or know that a child is being negatively impacted by things happening to them online, consider seeking professional support for them.

Kids Helpline
Kids Helpline service provides free, confidential online counselling for children and young people. Kids Helpline also provides young people experiencing problems online with free and private web chat counselling.

kidshelpline.com.au or phone 1800 55 1800

eHeadspace
eHeadspace is a confidential, free and secure space where young people aged 12 to 25 or their family can chat, email or speak on the phone with a qualified youth mental health professional.

eheadspace.org.au

Resources

Parentline
Parentline provides a counselling, information and referral service for parents that operates seven days a week between 8am and 10pm.

parentline.com.au or phone 1300 30 1300

Lifeline
Lifeline provides free 24-hour crisis counselling and information about support services.

lifeline.org.au or phone 13 11 14.

Crime Stoppers
Crime Stoppers or your local police can assist with concerns about children’s personal safety.

crimestoppers.com.au or phone 1800 333 000

The Office of the Children’s eSafety Commissioner
The Office’s website contains information and related links to support parents in keeping kids safe online. Resources include practical, action focussed advice, videos, games, support, and research-based information, and everything is free of charge.

esafety.gov.au

School support
Many schools have detailed policies and procedures in place to help support children online, including how to manage issues like cyberbullying, sexting and other online concerns.

The Department of Education policies in each state provide information for students, teachers, parents and the broader community to help raise awareness and counter the inappropriate use of technology.

For more information, contact your child’s school.

The Office of the Children’s eSafety Commissioner
The Office’s website contains information and related links to support parents in keeping kids safe online. Resources include practical, action focussed advice, videos, games, support, and research-based information, and everything is free of charge.

esafety.gov.au

Help and resources

Check out the following support services and resources to help you keep your family safe online.
Let’s get social

You can stay up-to-date with the latest online safety news, advice and resources on our social media channels:

Blog
esafety.gov.au/eSafetyblog

Facebook
facebook.com/eSafetyOffice

Twitter
@eSafetyOffice

YouTube
youtube.com/c/OfficeoftheChildrensSafetyCommissionerAU
Office of the Children's eSafety Commissioner

Australian Government