



Communications and Media Authority

cyber(smart:)

Parents' guide to online safety

Practical, issue-focussed information and advice for parents of children of all ages.



Cybersmart is a national cybersafety education program managed by the Australian Communications and Media Authority (ACMA) as part of the Australian Government's commitment to cybersafety. The program is specifically designed to meet the needs of children, young people, parents and teachers.



cyber(smart:)

Cyberbullying



Cyberbullying is the use of technology to bully a person or group. Bullying is repeated behaviour with the intent to harm others. Behaviour may include:

- + Abusive texts and emails
- + Posting unkind or threatening messages, videos or images on social media websites
- + Imitating or excluding others online
- + Inappropriate image tagging

For many teenagers, their online life is an important part of their social identity. Many young people fear that parents might take away their devices and refuse access to the internet and so do not report cyberbullying to their parents. Teenagers are also often concerned that parents' actions will make cyberbullying issues worse, so it is important to remain calm and supportive.

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. Work out strategies to address any potential issues and reassure your child that you will be there to support them.
- Advise your child not to reply to any messages from a bully. Often if bullies don't receive a response they will give up.
- + Learn how to block a bully so they are no longer able to make contact.

- Keep a record of harassing messages in case authorities become involved. Put them somewhere your child won't continue to see them.
- Contact the website administrator or use the reporting function to ask for content to be removed or to report harassment.
- Talk to your child's school if cyberbullying involves another student. The school should have a policy in place to help manage the issue.
- + 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, including through the Cybersmart Online Helpline at cybersmart.gov.au/ report.aspx

Social Networking

Social networking describes a variety of services like Facebook, YouTube, Instagram, World of Warcraft, Moshi Monsters, Twitter, Skype, Snapchat, 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 teenagers.

GROOMING

Online grooming is the illegal act of adults making contact with a child online for the purpose of establishing a sexual relationship. Often this will be via a social networking site, but it may also be through other online services.

WHAT CAN I DO? As a parent, you can help your child have positive experiences on social networking sites.

- Stay involved in your child's use of new 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!
- + Check the age restrictions for the social networking service or game. Some social networking sites (such as Club Penguin) are created especially for children under the age of 13, but most mainstream sites like Facebook, Instagram and others require the user to be 13 or older.
- Advise children to set their accounts to private so that only people they want to see it can view their information.
- + Encourage children to think before they put anything online. Information posted online can be difficult or impossible to remove. An inappropriate image posted today can have a long term impact on their digital reputation.
- + Show them how to set up location services on their phone so they are not inadvertently broadcasting their location.

- Remind children to be careful when making new friends online; people may not be who they say they are. Never arrange to meet an online friend unless a trusted adult is with them.
- Report any abuse or inappropriate content to the social networking site and show children how to do this too.
- Learn how to keep a copy of online conversations and how to block people prior to an issue occurring.

For more information on managing your children's access to particular social networking sites, visit cybersmart.gov.au/parents.aspx

Sexting

Sexting is the sending of provocative or sexual photos, messages, or videos, generally using a mobile phone or webcam. It can also include posting this type of material online. Young people often consider sexting as a

way of connecting in a relationship.

While sharing suggestive images or text messages may seem like innocent flirting or fun, sexting can have serious social and legal consequences. To help protect their reputation, young people need to consider what they share online, and how they handle messages and images sent to them by others.

In most instances of sexting, young people willingly share naked photos of themselves. However sexting can also happen in response to peer pressure. Accidents can also occur; for example, the sender or receiver of sexts may have their phone stolen by someone who decides to publish the images online.

- Talk to your child about sexting to prevent any issues from arising.
 Make sure they are well aware of the risks that may occur if their images were to be spread beyond the person they intended them for.
- Remind your child about the social and legal consequences of sexting. If anyone in the photo or video is under 18 they may be committing a crime if they send, receive or forward messages.
- 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.
- Try to get the image/video removed from all locations to the greatest extent possible. If sexting content is posted online, report it to the website administrator.
- Seek help from the school if necessary. Ask them to help track who might have the image or video and where it might be posted. Ask them to provide support to your child and others involved.
- Ensure that your child is supported if they have been negatively impacted by sexting. Their friends are critical so try to help them stay connected to them for support, both online and offline.

Mobile Phone Safety

Mobile phones are a great way for children and teenagers to stay in touch with their parents, family and friends and provide access to fun and functional resources like games, the internet, music, apps and more from anywhere at any time.

Many young people would never be without their mobile phone, and a mobile phone provides you with immediate access to your children. However, the fact that they are 24/7 and you can't always be there to supervise means there are potential risks. These can include high or unexpected bill costs, cyberbullying, sexting, broadcasting their location to unintended others through 'checking in' and access to inappropriate material.

- If you think your child needs a mobile phone, consider purchasing a phone that is not internet enabled. Smartphones come with features you may not yet want your child to have such as unsupervised internet access, a camera, and a wide variety of online games and apps.
- Stay involved with your child's use of their mobile phone. If you don't have a good understanding of how their phone works and what they use it for, ask them to show you.

- Help your child to understand that they should treat their phone like a wallet, and that every text message, phone call or download costs money.
- Let your child know that it's ok to tell you if they come across something that worries them, and that their phone won't be taken off them if they report something to you.
- Investigate phone plans and pre-paid contracts. Decide what your child needs from their mobile phone so you are well-educated on options before you approach a provider.

- Check automatic download settings and in-app purchase settings on your child's mobile phone, as these can incur extra costs or use up credit quickly.
- Consider keeping credit card details away from your children so music and apps cannot be purchased without your knowledge. If you have your credit card details stored on an online account, you may choose to keep the password to this account private.

Offensive or Illegal Content+



Children and young people may not deliberately seek out inappropriate content. Children can inadvertently access disturbing or illegal content while undertaking online searches or by clicking on unknown links.

Offensive or illegal content may include topics, images or other information that are prohibited in Australia or could be damaging to young people online. 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 and 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 terrorist activities

- + Be aware of how your child uses the internet and explore it with them. Discuss the kinds of sites that are ok to explore and those that are not.
- consider using parental controls such as filters to help manage your child's online access.
- Remind your child not to open spam email or click on pop ups, prize offers or unfamiliar hyperlinks in websites.

- Help your child use search engines to locate websites. Consider developing a list of favourites for younger children. Enable safe search options.
- Reassure your child that access to the internet will not be denied if they report seeing inappropriate content to you.
- Remind them not to respond if they are sent something inappropriate and that they should leave a website immediately if they feel uncomfortable or worried.
- Report content that you think may be prohibited to the ACMA's online hotline: acma.gov.au/hotline



How much is too much?

Your child may be spending too much time online if their online behaviour is having a negative impact on other aspects of their life.

To many parents it can seem as though children and young people are constantly online. Often they are multitasking; for example downloading and listening to music while studying and chatting with friends or sending messages on their mobile phones.

The number of hours 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 behaviour 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.

- 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 filter on the laptop or computer 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. You might like to have a rule where the 'wifi password of the day' is only given once all homework/chores/family time is done. 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. Consider getting help from school counsellors or your GP who can refer your child to a professional psychologist.

Help and Resources

Check out the following support services and resources to help you keep your family safe online.

- The Cybersmart 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.
 Visit cybersmart.gov.au
- + Cybersmart Outreach offers free, school based presentations to keep parents, students and teachers up-to-date with cybersafety issues. These sessions are informative, non-technical and available to all schools. Ask your child's school if they have registered to host a presentation.

Visit cybersmart.gov.au/outreach.aspx

- + School support Schools may have detailed policies and procedures in place to help support children online, including how to manage issues like cyberbullying, sexting and other online concerns. For more information, contact your child's school.
- + 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 including through the Cybersmart Online Helpline, provided by Kids Helpline. The service provides free, confidential online counselling for children and young people.

Visit cybersmart.gov.au/report.aspx

+ The Department of Communications' Easy Guide to Socialising Online, provides information on the safe use of social networking sites, games and search engines. Visit



Cybersmart, through Kids Helpline, also provides young people experiencing problems online with free and private web chat counselling.

(h) cybersmart.gov.au/report.aspx

1800 55 1800

All of Cybersmart's information, games, videos and teacher resources are available free-of-charge from cybersmart.gov.au

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

Social

- acma.gov.au/Cybersmartblog
- f facebook.com/cybersmartcloud
- @CybersmartACMA
- You Tube ACMACybersmart

Contact us

- cybersmart@acma.gov.au
- 1800 880 176

cyber(smart:)