Australian Government

acma
Australian Communications and Media Authority

cyber(smart:)

Cyberbullying

Teenagers

Cyberbullying occurs when the internet, email or mobile phones are used to deliberately an repeatedly engage in hostile behaviour to harm someone. Cyberbullying occurs most commonly among older children and teens.

Cyberbullying can have negative academic, social and psychological outcomes, so providing support for children and young people who are involved in cyberbullying is critical.

For many teens, their online life is an important part of their social identity. Many teens fear that parents might disconnect them from the internet and therefore their supportive friends as a 'solution' to cyberbullying. This prevents some teens from reporting cyberbullying issues. Some teens are also concerned that parents will make cyberbullying issues worse.

To help teens deal with cyberbullying:

- Talk to your teen about cyberbullying before it happens. Work out strategies to address cyberbullying that you are both comfortable with, so your child knows what to expect if they do report concerns to you or another trusted adult. Reassure them that you are will be there to support them and won't disconnect them from their online world.
- Encourage your teen to tell you or another trusted adult if they receive or hear of negative messages, or are excluded by others. Help them stay connected to trusted friends and family both online and offline. This is an important protective measure against the potentially negative outcomes of bullying.
- Advise your teen not to respond to any negative messages but to save the messages and details of the senders. You may want to save the messages for your teen so that they don't keep reading them and potentially feel worse.
- You can help your teen report any concerns to the administrator of the service used, including the mobile phone provider (if SMS is involved), website administrator (if social networking or chat services are involved), or internet service provider.
- Understand your school's policy about cyberbullying—do they have a policy and what is the likely outcome of a complaint about cyberbullying if another student is involved.
- Encourage your teen to support their friends and report concerns about friends who may be involved in cyberbullying.
- Advise your child never to share their password with friends—friendships may be shortlived at this age and former friends can mis-use passwords to cyberbully.
- 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 www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people. Your child's schools may also be able to provide support and guidance.
- If there is a threat to your child's safety the police can help. In life threatening and time critical situation call Triple Zero (000).

Australian Government

acma
Australian
Communications
and Media Authority

cyber(smart:)

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Digital reputation

Teenagers

All internet users will have a digital or online reputation. Essentially, this digital reputation is the opinion that others hold about the user. Children should be encouraged to think about their digital reputation when interacting online. Digital reputations are informed by content that is posted online and how people communicate online. People can be judged on how they behaved as a teenager well into the future. The following tips can help teens understand and manage their digital reputations.

- Talk to your teen about managing personal information on social networking sites. Encourage them not to put any personal information on their profiles. This includes their phone number, personal email address, home or school addresses, or the name of their school.
- Encourage your teen to be careful when they post photos and to consider how what they post might be viewed by others.
- Talk to your teen about the potential social, academic, employment and legal implications of posting inappropriate material of themselves or others online. Encourage them to think about who might see the content and what the impact might be now and in the future.
- Remind your teen that much of what they do online can be made public, and may go beyond the group of friends they intend it to reach. A good general guide is for teens not to post photos that they would not want strangers to see.
- Help your teen understand that information they provide online or via SMS can be shared more broadly than they might think. Even if their profile is set to private, they can't control what their friends will do with the information hey post. Encourage them to think carefully before sharing images or controversial messages online or via mobile.
- Remind your teen to take care with others' digital reputations. They should not post images of others without their permission and should take care with comments about others.
- Ensure teens understand the features and terms of use of social networking sites—in particular how to set their profile to private.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Australian Government

acma
Australian Communications and Media Authority

cyber(smart:)

Excessive internet use

Teenagers

Many teens spend a fair amount of time on the internet socialising, studying and for entertainment. For many their online activities form a part of their social identity. However, it is important that teens take care of themselves and balance their online interactions with other aspects of their lives.

There are no guidelines for the ‘right’ amount of time for teens 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 agreed time limits on use.

The following tips can help teens to manage time spent online and help them to maintain a healthy balance.

- Look for indicators that your teen may be spending too much time online, such as a decline in interest in other activities, talking constantly about an online game or activity, a decline in grades or irritability when they are away from a game. You may also suspect they are getting up after bed time to play games or chat to others.
- Teens may seem quite tired during the day or skip meals to avoid leaving the computer.
- You may like to check with your teen’s school to identify whether they are experiencing issues with timeliness or quality of work.
- If issues arise consider establishing rules about when teens can play games or use the internet and how long they can play each day. You might consider agreeing with your teen a set balance of online and offline activities. You may need to establish consequences for rule breaches. For example, if your teen doesn't undertake their assigned jobs they may have access to online games restricted.
- Try to locate the computer in a shared or visible place in the home so you are aware of how much time your teen spends online.
- If you have concerns about your teen’s online behaviour explore your concerns with them. If necessary seek professional support, including support through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people. Your teen’s school may also be able to provide guidance and support.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Identity theft

Teenagers

Identity theft is a specific type of fraud, which involves stealing money or gaining other benefits by pretending to be someone else. Identity theft can be devastating—both financially and emotionally. It can occur in many ways—from somebody using credit card details illegally to make purchases, to having a person's entire identity assumed by another to open bank accounts, take out loans and conduct illegal business under that name.

Teens need to consider the potential for their personal information to be accessed and misused by others on the internet and to take protective measures to protect their information. The following tips can help teens manage their personal information.

- Encourage teens to delete emails from unknown sources and not to open attachments in such emails. These may contain malicious software which can compromise computers.
- Encourage teens to establish a separate email account that can be used to sign up to websites. This account will be separate to all other personal accounts so it can easily be deleted if it is misused.
- Consider using filters, labels and safe zones to help manage your teen's online access.
- Install and update anti-virus and other e-security software to restrict unauthorised access to data on the home computer and protect that data from corruption. Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks.
- Encourage teens not to download files or applications from suspect websites. The file or application could contain malicious software which can compromise computers.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Legal downloading

Teenagers

Downloading is popular with teens who may download media files such as music, TV shows, movies and ringtones. The following tips can help guide your teen to download safely.

- Talk with your teen about the potential risks of using unsafe websites to download and share files, including the risk of infecting the home computer with viruses, the potential costs and the legalities of breaching copyright.
- If you want to teach your teen about downloading use a reliable and legal media download site such as the ABC's iView.
- If you are unsure about other safe or legal websites to use ask around—word of mouth from friends and family is a good way to identify reliable download sources.
- If you are comfortable with your child using download sites that charge for use you might consider visiting your preferred websites with them and checking the fees. It may be useful to establish rules requiring your child to seek your permission before they download files, to prevent unexpected costs. Establishing a weekly family budget for media downloads can help.
- If your child uses a download site that charges fees check that the website has secure online payment facilities. Look for a https:// in the address field and a locked padlock symbol at the bottom of the screen. The https:// and padlock indicate that financial data is being encrypted and protected from unauthorised access.
- Talk to your child about the download limit of your internet contract. What is the limit and what is the cost if it is exceeded? What sort of usage occurs with each download, and how you can check current usage with your child?
- Consider using filters, labels and safe zones to help manage your child's online access.
- Install and update anti-virus and other e-security software to restrict unauthorised access to data on the home computer and protect that data from corruption. Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Australian Government

acma
Australian Communications and Media Authority

cyber(smart:)

Mobile phone costs

Teenagers

Many teens are enthusiastic mobile phone users and may have access to both their own, and their friends' mobiles. The following tips can help guide your teen in the safe and responsible use of mobiles.

- Stay involved with your teen's use of new technologies. Ask your teen to show you how their phone works. Warn teens not to post their number or anybody else's number online.
- If you are concerned about your teen's ability to manage their phone costs find out how access to 'adult' content and other services, such as premium SMS services or internet access, can be managed. This information is often available on the carrier's website.
- Look at the terms and conditions of mobile plans with teens to ensure they are aware of potential costs, particularly in relation to internet download costs. Comparing the different costs and download limits of contract and prepaid services will help you decide which service is best for you and your child.
- Help teens understand the potential costs of subscription services. Encourage them to check the terms and conditions before subscribing to a service, and to SMS the word 'STOP' if they wish to cancel a subscription service.
- Remind your teen that they shouldn't let anyone borrow their phone. Caution them to be wary of anyone who asks to borrow their phone in public—even if it's for a supposed emergency. They can dial Triple Zero (000) for the person in need.
- Teach your teen that they should not respond if they are sent something inappropriate, including sexting images, and they should immediately hang up if they feel worried.
- Encourage teens to report any unkind messages they receive to a trusted adult and to keep the messages in case follow-up is required with the phone provider or the police.
- Teens also should not reply to messages from unknown sources. These could be scams
- If your teen has incurred excessive costs contact your mobile phone provider in the first instance. The Telecommunications Industry Ombudsman may also be able to help.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Offensive or illegal content

Teenagers

Teenagers may see come across offensive online content by accident or they may seek it out. The following tips will help teens manage the content they access online.

- Be mindful that some websites encourage harmful or illegal behaviours such as eating disorders and violent acts. Consider your teen's vulnerability to information and check what they are viewing online.
- Try to have the computer in a shared or visible place in the home, particularly if your teen is vulnerable; for example, has a mental health issue or behavioural issue.
- Teach your teens that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and tell a trusted adult if they feel uncomfortable or concerned about themselves or a friend.
- Reassure teens that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for teens that may stop them from communicating with you openly.
- Encourage your teen to look out for friends. If they know a friend is accessing content that seems to be impacting on them negatively encourage them to share their concern with their friend and report it to a trusted adult anonymously if necessary.
- If your teen is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support, including through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.
- Your child's school may also be able to provide assistance or guidance.
- Consider using filters, labels and safe zones to help manage your teen's online access.
- Report content that you think may be prohibited to the ACMA's Online Hotline at www.acma.gov.au/hotline.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Online purchasing

Teenagers

Teenagers may make online purchases or use internet banking. It's important that teens understand how to identify websites with secure payment facilities and how websites can use banking details and other personal information unsafely. The following tips can help your teen understand and manage the risks of purchasing online.

- Advise your teen to only use trusted sites when making online purchases. They should check that the website has secure online payment facilities identified by a https:// in the address field and a locked padlock symbol at the bottom of the screen. This indicates financial data is being encrypted and protected against unauthorised access.
- If using online auction sites, ask teens to check the reputation of the seller prior to purchase. Check seller and product reviews as well.
- Advise your teen that they pay attention to their intuition if they have doubts about the legitimacy of a website or email requesting financial details or payment. They can call the organisation a website or email claims to represent to check the legitimacy. When calling, your teen should not use phone numbers provided on the suspect website or in suspect emails. They should use a known phone number or one obtained from a trusted source such as the White or Yellow Pages or a government website.
- Encourage your teen to check all costs including handling fees, delivery options and charges and warranty conditions.
- Check bank statements regularly after your teen makes an online purchase to ensure no anomalies appear. If they do, help your teen contact their financial institution immediately.
- Encourage your teen to check the small print before agreeing to a service. Some services teens favour such as game downloads for mobile phones may be ongoing rather than a one off purchase, with a new game provided weekly at a cost until 'STOP' is sent to the content provider.
- Advise teens to be wary of offers that seem to good to be true—they usually are. If concerned that your teen may have been the target of a scam, for example, if they paid for an item but didn't receive it, contact your local consumer affairs agency or visit the Scamwatch website at www.Scamwatch.gov.au. If they provided personal or financial information, contact local police and your financial institution directly.
- Install and update anti-virus and other e-security software to restrict unauthorised access to data on the home computer and protect that data from corruption. Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Australian Government

acma

Australian Communications and Media Authority

cyber(smart:)

Protecting your information

Teenagers

Personal information is any information or combination of information that enables the identification of an individual.

Personal information is disclosed to, and used responsibly by, many legitimate online businesses to conduct business and online social interactions. However, if not managed carefully, it is possible for personal information to be accessed and misused for marketing, identity theft or for cyberbullying or cyberstalking.

The following tips can help teens manage their personal information safely and responsibly.

- Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams, to steal their identity or worse.
- Talk to your teen about managing personal information on social networking sites. Encourage them not to put any personal information on their profiles. This includes their phone number, personal email address, home or school addresses, or the name of their school.
- Encourage your teen to be careful when they post photos that they are not accidentally providing clues to personal information such as their school uniform.
- Encourage your teen to set up a separate email account for use when signing up to games or websites. This account will be separate to all other personal accounts so they can disable it if it's misused. It should not include their names or other identifiers in the address.
- They might also like to set up a separate social networking account if they want to promote themselves or an interest and engage with like minded people that they don't know offline. They should ensure the site does not contain their personal information.
- Encourage your teen to read user agreements and privacy policies to determine how their personal information may be used when signing up to services as many organisations use information for their own marketing and some sell it to other marketing firms.
- Remind your teen that they should only disclose financial information on websites that they trust and that have secure payment facilities identified by a web address beginning with https:// and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.
- Remind your teen that banking institutions will never email individuals asking for their user name or password. If they receive an email from an organisation claiming to represent a banking institution they should report the email to the bank and the Government's SCAMwatch website at www.scamwatch.gov.au or their local consumer affairs agency. They should not respond and not click on any links provided.

Australian Government

acma

Australian Communications and Media Authority

cyber(smart:)

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Safer social networking

Teenagers

Social networking describes a variety of online services like Facebook, YouTube, Foursquare, Twitter and online games such as World of Warcraft and Runescape. These services let children and teens communicate with other people online. This can enable children and teens to stay in touch with friends and family. However, teens may disclose too much information online. They may also behave in ways that they wouldn't offline. The following tips will assist teens to behave safely when using social networking.

- Talk to your teen about managing personal information on social networking websites. Encourage them not to put key personal information on their profiles. This includes their phone number, home or school addresses, information about workplaces or clubs.
- Remind your teen not to post photos of themselves or others that they would not want strangers to see, or that may have a negative impact on how others view them.
- Ensure your teen understands the privacy features—in particular how to set their profile to private and limit access to their information. Encourage teens to screen online 'friends'.
- Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams or cyberstalking.
- Talk to your teen about the use of location based services. Services such as Foursquare and Facebook enable social networking users to report their physical location to other users by 'checking in'. Some services let people report their friends' locations and have location based functions turned on by default. Your teen can review their settings and block this function or limit who sees their location based information. Remind your teen that allowing strangers to see where they are**,** or where their mates are, is a risky behaviour.
- You may also like to contact your mobile phone company for assistance with blocking internet, Bluetooth and GPS functionality on their child's mobile phone to limit their ability to notify others of their whereabouts.
- Encourage your teen to keep their online friends online. If they do want to meet someone that they haven't met so far in person, they should ask a parent or another trusted adult to go with them and always meet in a public place, preferably during the day.
- Remind your teen not to respond if someone sends them negative messages or asks them to do something that makes them feel uncomfortable. They should tell a trusted adult and save the messages.
- Encourage your teen to set up a separate social networking account if they want to promote themselves or an interest and engage with like minded people that they don't know offline. They should ensure the site does not contain their personal information.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Australian Government

acma
Australian
Communications
and Media Authority

cyber(smart:)

Unwanted sexual contact

Teenagers

Some adults befriend children online for sexual purposes. This is called grooming. It is illegal and should be reported to police. In many cases police can prosecute adults seeking children for sexual purposes even if they haven't made face to face contact with a child.

Many teens use sites that allow them to directly interact with people they don't know offline. There is a risk that the individuals teens connect with may not be who they claim to be, or that they intend to establish a sexual relationship with your teen. The following tips can help guide your teen's behaviour and help keep them safe from unwanted sexual contact.

- Stay involved in your teen's use of new technologies—keep up to date with the websites they are visiting and explore them with your teen if possible. In general it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others including adults.
- Remind your teen to create screen names or IDs that do not indicate gender, age, name or location and are not sexually provocative.
- Guide your teen to use their privacy settings to restrict their online information to viewing by known friends only.
- Encourage your teen to keep their online friends online. If they want to meet someone that they haven't met in person encourage them to ask a parent or another trusted adult to go with them and always meet in public places, preferably during the day.
- Encourage your teen to be alert to people online who make them feel uncomfortable and to block them. They should report inappropriate contact to the website administrators.
- Some teens feel worried about their parents' reaction to things they may have said or done online, especially if they think they encouraged online sexual contact. This can prevent them reporting concerns about online contacts. Perpetrators play on this worry and shame to isolate teens from family and friends and encourage teens to trust and confide in them.
- To overcome this risk reassure your teen that you will always support them and not block their internet access if they report that they are uncomfortable or worried about what somebody has been saying online.
- Be alert to changes in your teen'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 support including through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people. Your child's school may also be able to provide guidance and support.

- If there is a threat to your child’s safety the police can help. In a life threatening and time critical situation call Triple Zero (000).

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.

Australian Government

acma
Australian
Communications
and Media Authority

cyber(smart:)

Violent content

Teenagers

Teens may come across violent content while they are online. This could be through video games, video sharing websites or other images. The following tips can help teens manage the content they access online.

- Encourage teens to check game classifications prior to game purchase. Every child reacts differently to violent content so consider game content before agreeing to let your teen use it. You may wish to veto games that you feel don't meet family standards or are unsuitable for your child.
- Consider setting rules about game usage within the home including frequency and types of games.
- Try to have the computer in a shared or visible place in the home. Ensuring gaming access is in public areas of the house rather than bedrooms provides some insight into what your teen is doing and an opportunity to talk with them about their activities online.
- Report content that you think may be prohibited to the ACMA's Online Hotline at www.acma.gov.au/hotline.
- If your teen is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support, including support through the Cybersmart Online Helpline at www.cybersmart.gov.au/report.aspx. The Cybersmart Online Helpline provides free, confidential online counselling for children and young people.
- Your teen's school may also be able to provide assistance or guidance.
- Consider using filters, labels and safe zones to help manage your child's online access.

More information

The Cybersmart program provides a range of cybersafety materials for parents and their children. For more information, resources, advice and tips, visit the Cybersmart website at www.cybersmart.gov.au. Encourage your children and teens to take a look around the website. If you have young children, you may like to explore it together to help them understand how to protect themselves against online risks and make the most of their experiences online.