Cyberbullying

Older children

Cyberbullying occurs when the internet, email or mobile phones are used to deliberately and 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. Helping children to manage responses to negative online behaviour and keeping them connected online and offline to friends and family that they trust are important measures to protect them from potentially negative outcomes.

The following tips can help you to manage cyberbullying with your child.

- At this age your child's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Talk to your child 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 your child that you won't block their access to the internet if they report concerns about cyberbullying. Help them to stay connected online and offline to supportive family and friends.

- Help your child to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly,

- Advise your child 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 child so that they don't keep reading them and potentially feel worse.

- Encourage children to support their friends and report concerns about friends who may be involved in cyberbullying.

- Help your child to develop the skills they need to interact safely and respectfully online. Guide their online activities and help them learn to communicate appropriately with friends and family.

- 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).

More information

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.

Excessive internet use

Older children

Many older children spend time on the internet socialising, studying and for entertainment. 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 online time limits.

To following tips can help your child manage time spent online and maintain a healthy balance.

- Look for indicators that your child may be spending too much time online, such as declining interest in other activities, talking constantly about an online game or activity, a decline in grades or irritability when they are away from an online game. You may also suspect they are getting up after bed time to play a game.

- Children may seem quite tired during the day or skip meals to avoid leaving the computer.

- You may like to check with your child's school to identify whether they are experiencing issues with timeliness or quality of work, and tiredness.

- Consider establishing rules about when children can play games or use the internet and how long they can play each day. You might consider agreeing with your child a set balance of online activities and offline activities such as outside play, homework and housework. A two week trial of new rules might be useful to establish whether they seem to provide a good balance for your child and your family.

- Establishing rules with children when they are young can help with the management of their online activities as they get older.

- Try to locate the computer in a shared or visible place in the home so you are aware of how much time your child spends online.

- If you have concerns about your child'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 child'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

Older children

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.

Children's online use is likely to put them at little risk of identity theft. However, the following tips provide guidance to help teach children to protect their personal information and yours.

- At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Encourage your child to tell you about new websites and games that they like and explore them together. Check whether personal information is required to sign up to new websites or games and help your child sign up if you feel it is appropriate.

- Talk to your child about personal information and why it is special. This sort of information can be used to identify or locate where they live, go to school or activities in which they are involved.

- Set rules—make sure your child knows what information they can share or post online and which websites they can visit. Telling a trusted adult before posting any personal information online, including for competition entry, is a useful rule.

- Consider creating a family 'fun' email account that can be used for competition entries and other activities. 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 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.

Legal downloading

Older children

Downloading can start to be a risk for older children who are interested in downloading media files such as music, TV shows, movies and ring tones. The following tips can be used to help you to guide your child.

- Talk with your child 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 child 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.

Mobile phone costs

Older children

Older children may have their own phone, use their parents' phone or have access to those of their friends. The following tips can help guide children in the safe use of mobiles.

- Stay involved with your child's use of new technologies. Ask your child to show you how their phone works and what they use it for. Warn your child not to post their number or anybody else's number online. Encourage them to tell you if they run into any trouble with their mobile phone.

- Help your child to understand that every text message, phone call or download service costs money. It may be useful to establish rules about when they are allowed to use their phone and for what. A monthly spend limit may also be useful.

- If you are concerned about your child'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.

- You may also like to consider using a prepaid service for your child which will enable you to limit costs more easily. 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.

- If your child has subscribed to a premium service (like a ringtone download) and they want to stop their subscription help them SMS the word 'STOP' to the service provider.

- Remind your child that they shouldn't let anyone borrow their phone. Caution them to be wary of anyone who asks to borrow your phone in public—even if it's for a supposed emergency. They can dial Triple Zero (000) for the person in need.

- Teach your child that there are ways they can deal with material that worries or frightens them—they should not respond if they receive an inappropriate phone call or message, and they should immediately hang up and tell a trusted adult if they feel uncomfortable.

- If your child 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

Older children

Older children may come across offensive online content by accident or they may seek it out with encouragement from peers. The following tips can help older children to manage online content.

- At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Discuss the type of content that is and isn't okay online including violent or rude content. This will depend on your family standards.

- Teach your child that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and they should tell a trusted adult if they feel uncomfortable or worried.

- Reassure your child 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 children that may stop them from communicating with you openly.

- Teach your child how to close web pages that they don't like or to turn off the monitor and call a trusted adult.

- If your child 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 child'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

Older children

Children are unlikely to make purchases online without the advice and guidance of their parents, but may be more keen to with age. Some gaming websites charge for additional features, and many legal music download sites also have charges per download. It is important for parents to have a good understanding about their children's interests and how to purchase online safely. The following tips can help to guide online purchasing.

- When making online purchases, only use trusted sites. 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 to identify secure sites. This indicates financial data is being encrypted and protected against unauthorised access.

- If using online auction sites, check the reputation of the seller prior to purchase. Check seller and product reviews as well.

- If in doubt about the legitimacy of a website or email requesting financial details or payment, call the organisation it claims to represent to check. When calling, do not use phone numbers provided on the suspect website or in suspect emails. Use a known phone number or one obtained from a trusted source such as the White or Yellow Pages or a government website.

- When you are making a purchase check all costs including handling fees, delivery options and charges and warranty conditions.

- Check bank statements regularly after making an online purchase to ensure no anomalies appear. If they do, contact your financial institution immediately.

- Check the small print before agreeing to a service. Some services children 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.

- Be wary of offers that seem to good to be true—they usually are. If concerned that you may have been the target of a scam, for example, if you 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 you 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 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.

Protecting your information

Older children

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.

The following general guidelines are a useful starting point to teach older children to use their personal information safely and responsibly online.

- At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Check whether personal information is required to sign up any of their favourite websites or games and help your child sign up and use privacy settings safely if you feel it is appropriate.

- Talk to your child about personal information and why it is special. This sort of information is information that can be used to identify or locate them and where they live, go to school or join in activities.

- Set rules—make sure your child knows what information they can share or post online and which websites they can visit. Telling a trusted adult before posting any personal information online, including for competition entry is a useful rule.

- Remind your child that not everybody online is who they say they are and encourage them to be cautious when sharing information.

- Help your child to create screen names or IDs that do not communicate their gender, age, name or location.

- Consider creating a family 'fun' email account that can be used for competition entries and other activities. This account will be separate to all other personal accounts so it can easily be deleted if it is misused.

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

Older children

Social networking describes a variety of online services like Facebook, YouTube, MySpace, Twitter, online games such as World of Warcraft and Moshi Monsters and virtual worlds such as Club Penguin. Some social networking sites targeted at children claim to moderate or check communication to provide greater protection for children.

Social networking services let children and teens communicate with other people online. This can enable young people to stay in touch with friends and family and join in fun fantasy worlds and games. However, children may forget who they are communicating with online and disclose too much information. They may also behave in ways that they wouldn't offline.

The following tips can assist in managing children's social networking interactions

- If your child is using social networking services check the website age guidelines and terms and conditions. In general it is useful to consider whether you are comfortable with the content and the potential for contact with others including teens and adults. Is your child socially ready to manage contact from potentially ill meaning strangers?

- Help your child set up their profile to make sure that they don't put too much personal information online. Help your child to create screen names or IDs that do not communicate their gender, age, name or location and are not sexually provocative.

- Set rules—make sure your child knows what information they can share or post online. Ask them to tell you before joining new websites and before they post any personal information online, including their full name, address or school.

- Advise your child not to respond to any negative messages and to report any negative messages they receive to you or another trusted adult.

- Establish rules around the type of contact they should report to an adult. For example, one rule may be 'tell Mum if somebody asks you about your underwear or private parts'.

- Reassure your child 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 children that may stop them from communicating with you openly.

- Advise your child to check with you before clicking on links sent by others on social networking websites. These may lead to adult content.

- Remind your child to communicate appropriately with others online, and to report any bullying of themselves or others to you or another trusted adult.

- Talk to your child about the use of location based services. These services 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 child can review their settings and block this function or limit

who sees their location based information. Remind your child 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.

- 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.

Unwanted sexual contact

Older children

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.

Older children may become more interested in websites and gaming sites that enable direct interaction with others including teens and adults. The following tips can help to protect your child against unwanted sexual contact.

- At this age children's internet use should be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Explore your child's favourite websites. 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 teens and adults. Is your child socially ready to manage contact from potentially ill meaning strangers?

- If you agree to your child accessing sites which may allow direct contact with others consider establishing rules about the amount of information they can provide, including not providing their surname, address or school, and not uploading or SMSing images or videos without parental permission.

- If your child is at an age where you have begun educating them about strangers and protecting their body it may be useful to expand those lessons to cover online contact. The appropriate age for this education will vary and is a decision for you and your family.

- It may be useful to make a rule about what is and isn't okay to discuss on the computer and what should be reported to you or a trusted adult. For example, one rule might be 'if anyone asks you about your underwear or private parts when you are on the computer get Mum to check that what they are saying is okay'.

- Some children feel worried about their parent's reaction to things they may have said or done online and this can prevent them reporting genuine concerns. Perpetrators play on this worry and shame to isolate children. To overcome this reassure your child that they can always safely tell you that they feel uncomfortable or worried about what somebody has been saying to them and what they might have been saying and doing in response.

- If your child shows changes in behaviour or mood that are concerning including increased or decreased sexualised behaviours, clinginess or withdrawal 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. If of school age, 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.

Violent content

Older children

Older children may see a range of violent content while they are online. This could be through video games, video sharing websites or other images. This can be quite frightening for some children or may impact on their behaviour and perception of what is appropriate. The following tips will help older children manage the content they access.

- At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

- Be aware of how your child uses the internet and explore it with them. Bookmark a list of 'Favourites' you are comfortable with your child visiting and teach them how to access this list.

- Check age guidelines on the games and websites your child likes and consider whether they are old enough to understand the content, and whether they understand the difference between fantasy and reality. It is also important to consider whether content is suitable for your child and meets your family's content standards.

- Teach your child that there are ways they can deal with material that worries or frightens them—they should not respond if they receive something inappropriate, and they should immediately tell a trusted adult if they feel uncomfortable.

- Consider setting rules about game usage within the home, including frequency and the types of games.

- If your child 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 child's school may also be able to provide assistance or guidance.

- Report content that you think may be prohibited to the ACMA's Online Hotline at www.acma.gov.au/hotline.

- 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.