Cyber Safety Parent Information

St Bede's College, Mentone

The documents in this booklet are a starting point only for information on Cybersafety and ICT related problems. Links can be found on the College Website under Parent Portals to many more resources that are available for parents to use.

The attached documents are mainly from the ACMA website.

An online Cybersafety course called Connect.ed is an option if you want to learn more. See below for the link to enrol.

http://www.cybersmart.gov.au/Schools.aspx

connect.ed

http://acma.janison.com/acma/Default.aspx

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).

Technologies used for cyberbullying

The following listing provides information about technologies used for cyberbullying. For more information about technologies and sources young people are using, see the Current Technologies section of the Gateway.

Technology	Cyberbullying activities	Strategies for addressing this behaviour
Chat rooms message boards on the internet	• Sending or posting nasty or threatening messages which may be anonymous. • A group picking on or excluding individuals. • Misusing personal information gained by pretending to be someone's 'friend' to spread rumours, secrets and to gain power over others.	• Block communications with offensive individuals. • Don't respond to messages. • Keep a record of inappropriate postings, including time, date, user names for reporting. • Report misuse of personal information to the chat room or message board site host. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.
Emails and text messages via computer or mobile phone Instant Messaging (IM) on the internet	• Sending nasty or threatening messages or emails. • Forwarding offensive content including jokes, videos, images and sound. • Sending computer viruses. • Accessing someone else's account to forward personal emails or delete them. • Constantly calling or texting a person and making derogatory and/or rude remarks and/or threatening and hostile remarks. • Taking and sharing unflattering images with other mobiles or uploading onto the internet.	• Block communications with offensive individuals. • Don't respond to messages. • In the case of an SMS report misuse of the mobile phone to the phone company if known. • Keep inappropriate messages, including time, date, email addresses and mobile phone numbers for reporting. • If necessary create a new email address and only share it with close friends and family. • Ensure the computer is protected from compromise. Information is available in Protecting computers: e-Security in Common cybersafety issues in the

Technology	Cyberbullying activities	Strategies for addressing this behaviour
	• Using text or voice chat to harass or scare someone. • Sending a hostile attachment. • Using someone else's account to forward rude or unpleasant messages via their contacts list. • 'Ganging up'—a group deciding to pick on or exclude someone during IM.	Schools section on the ACMA Cybersmart website www.cybersmart.gov.au/schools.aspx. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.
Webcam	• Making and sending inappropriate pictures and content. • Persuading or threatening young people to act in inappropriate ways. • Using inappropriate recordings to manipulate young people.	• Block communication with people who make you feel uncomfortable. Turn off your webcam—claim it is broken if necessary. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.
Social networking sites on the internet	• Posting nasty and abusive comments. • Posting images, videos or sound that may embarrass or frighten a person. • Groups excluding a person from a network. • Creating a fake profile to bully, harass or create trouble for a person. • Accessing another person's account details and using their page to post negative materials, send unpleasant messages or make private information public.	• Ask the host site to remove any images, videos, etc, that are concerning. • Report inappropriate use of passwords, identity, etc, to the host site. • Keep a record of the actions of the offending parties, including the information posted, times, dates, any information about their username, etc. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.

Technology	Cyberbullying activities	Strategies for addressing this behaviour
Video hosting sites on the internet eg, YouTube	• Posting embarrassing or humiliating video clips.	• Ask the host site to remove the content. • Keep a record of the content and the ID of the person responsible for posting for reporting purposes. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.
Virtual worlds on the internet Gaming sites on the internet Playing games with people in your local area using handheld consoles	• Interacting negatively with someone else's avatar. • Pretending to be someone else's avatar. • Name calling and making abusive comments. • Picking on other users e.g. by repeatedly killing their characters or demeaning their lack of skill. • Denying access to a team game.	• Avoid interaction with the negative individual/group. • Report the issue to the game/virtual world site administrator. • Change avatar or character name if necessary. • Keep a record of the other player's avatars/usernames, their actions and the dates/times of their inappropriate behaviour for reporting purposes. • Report any incidence of bullying or upsetting hostile behaviour (including exclusion) to parents, school or a trusted adult or the Kids Helpline www.kidshelp.com.au or phone 1800 551 800.

Australian Government | acma Australian Communications and Media Authority

cyber(smart:)

Sexting

Teenagers

Sexting refers to the sending of sexual messages, photos or videos using a mobile phone. It can also refer to posting this type of material online. Involvement in sexting, or exposure to inappropriate imagery, is a very real risk for teenagers. The following tips can help guide teens in the choices they make when using mobile phones, web cams and sending messages.

- Talk with your teen about sexting and the social and legal consequences it can have.
- Sexting can have legal consequences if the images taken and shared are of minors. Even if all participants are willing, teens may be breaking the law if they take and share naked or sexual images of themselves or others who are minors. This is because sexting images may be considered child pornography.
- Sexting can have social consequences. For example, if images are forwarded on from the intended recipient, which has been the case following relationship break-ups, the social ramifications can be devastating for teens. Images may end up being viewed by many people through mobiles and posting of images online.
- Remind your teen to delete any sexual content they receive from others and to avoid forwarding this type of content.
- Remind your teen to consider the feelings of others when taking photos and distributing any content by mobile phone or online.
- Learn how to use your teen's mobile phone and talk with them about what they can and can't do with it.
- If you are concerned that a sexting incident may be a criminal matter, contact your local police.
- If your teen is exposed to inappropriate content or involved in creating such content talk with them about it. If necessary seek professional support, including support through the Cybersmart Online Helpline at http://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 or 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.

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.

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:)

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.

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.

Australian Government | acma Australian Communications and Media Authority

cyber(smart:)

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

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.

Australian Government | acma Australian Communications and Media Authority

cyber(smart:)

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

Australian Government | acma Australian Communications and Media Authority

cyber(smart:)

e-security—protecting your computer

e-security or internet security covers a range of activities to keep electronic information secure. Poor e-security or internet security can result in the corruption of files and can enable criminals and others to access personal and financial information.

The following tips can help you implement and maintain adequate e-security measures.

- **Use strong passwords.** Use long and random passwords for any application that provides access to your personal information, including logging onto your computer. Ideally, the password should be eight or more characters in length, not a dictionary word, contain a mixture of letters and numbers and contain a mixture of upper and lower case letters. Change passwords regularly and use different passwords for each application. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for practical advice on how to set and protect a 'strong' password. The Australian Computer Emergency Response Team's (AusCERT) website at www.auscert.org.au/ also provides a comprehensive reference guide to choosing good passwords.
- **Install and update anti-virus and other security software.** Viruses and other malicious software, such as worms and trojan horse viruses, can alter or erase data on your computers and allow spammers and other intruders to use your computer and network. Viruses and worms spread fast, and new variations are constantly being released, so anti-virus software must be updated regularly.
- **Anti-virus software** should be set to automatically scan all incoming and outgoing emails and any devices that are intermittently connected to a computer, such as a memory stick, a music player, digital camera, or other USB device. Set the software to automatically check for updates when connected to the internet. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for a guide to the installation and use of this software. The Internet industry Association at www.iia.net.au/ also provides relevant information.
- **Use a firewall and make sure it is turned on.** A firewall is your computer's first line of defence against intruders. Firewalls can block all traffic between your network and the internet that is not explicitly allowed, preventing unauthorised access to your data. A firewall should be used in conjunction with anti-virus and anti-spyware software. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for a guide to the use and installation of this software.
- **Manage emails safely.** Delete suspect emails immediately. If you do open an email that seems suspect, don't click on any links in the email. Visiting websites through clicking on links in suspect emails may result in malware (malicious software). This is a commonly used and effective means of compromising a computer. All email attachments should be scanned by anti-virus software before being opened. Anti-virus software can be set to do

this automatically. Use spam filtering software to manage unwanted emails and report spam to the ACMA. **Use safe internet browser settings.** When browsing the web, creating documents, reading email and playing games, using a limited permission account can prevent malicious code from being installed onto your computer. A 'limited permission' account is an account that does not have 'Administrator' status. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for a guide to the use of appropriate security settings for your web browser.

- **Keep up to date with security patches Most operati**ng systems are supported by automatic updates ('security patches') that fix vulnerabilities found in important software components. You should either use the 'automatic update' option, or subscribe to a security-related mailing list and install these patches when necessary.
- **Check and alter default settings.** After installing software, check the configuration and setting options—you may find the software has extra features you don't need or want. Turning off unnecessary services is a good security precaution.
- **Back up your data and files.** Back up your data regularly and check that backups are working. Creating a copy or backup of data is an effective way to help recover information from a computer if a virus destroys files, or the computer is stolen or destroyed. For example, burn data, photos, videos etc. on to a CD-Rom or a USB stick, or use an external hard drive regularly. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for a guide to backing up data.
- **Use caution when sharing or downloading files.** Don't download files or applications from suspect websites. The file or application could be malware. Sometimes the malware may even be falsely represented as e-security software designed to protect you. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for more information about sharing files safely.
- **Protecting wireless internet connections** Wireless networks require special attention to secure them from hijacking. Users should:
    - change the default password to a strong password
    - turn off the SSID broadcast on the wireless router
    - engage the highest level of encryption available for their wireless network, including turning the WPA encryption on
    - restrict access to the wireless network with MAC address filtering
    - monitor wireless networks for unusual activity
    - turn off the wireless connection when not in use.

Internet service providers or software vendors will be able to provide specific advice about protecting wireless networks. Visit the Secure your computer section of Stay Smart Online at www.staysmartonline.gov.au for a more detailed guide to securing wireless internet connections.

Keep up-to-date with security information. Users can keep up-to-date with security advice that affects their systems. Stay Smart Online at www.staysmartonline.gov.auprovides home users with information on the latest e-security threats through a free alert service. Reputable organisations such as: Australian Computer Emergency Response Team (AusCERT), operating systems (eg, Windows, MacOS, Linux) vendors, and anti-virus/security software vendors also provide security information about emerging threats to computer security.

Preventing Cyberbullying

Top Ten Tips for Parents

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.
Cyberbullying Research Center

1. Establish that **all rules for interacting with people in real life also apply for interacting online** or through cell phones. **Convey that cyberbullying inflicts harm** and causes pain in the real world as well as in cyberspace.

2. Make sure your school has Internet Safety educational programming in place. This should not solely cover the threat of sexual predators, but also how to prevent and respond to online peer harassment, interact wisely through social networking sites, and engage in responsible and ethical online communications.

3. Educate your children about appropriate Internet-based behaviors. Explain to them the problems that can be created when technology is misused (e.g., damaging their reputation, getting in trouble at school or with the police).

4. Model appropriate technology usage. Don't harass or joke about others while online, especially around your children. Don't text while driving. Your kids are watching and learning.

5. Monitor your child's activities while they are online. This can be done informally (through active participation in, and supervision of, your child's online experience) and formally (through software). Use discretion when covertly spying on your kids. This could cause more harm than good if your child feels their privacy has been violated. They may go completely underground with their online behaviors and deliberately work to hide their actions from you.

6. Use filtering and blocking software as a part of a *comprehensive* approach to online safety, but understand software programs *alone* will not keep kids safe or prevent them from bullying others or accessing inappropriate content. Most tech-savvy youth can figure out ways around filters very quickly.

7. Look for warning signs that something abnormal is going on with respect to their technology usage. If your child becomes withdrawn or their Internet use becomes obsessive, they could either be a victim or a perpetrator of cyberbullying.

8. Utilize an "Internet Use Contract" and a "Cell Phone Use Contract" to foster a crystal-clear understanding about what is appropriate and what is not with respect to the use of communications technology. To remind the child of this pledged commitment, we recommend that these contracts be posted in a highly visible place (e.g., next to the computer).

9. Cultivate and maintain an open, candid line of communication with your children, so that they are ready and willing to come to you whenever they experience something unpleasant or distressing in cyberspace. Victims of cyberbullying (and the bystanders who observe it) must know for sure that the adults who they tell will intervene rationally and logically, and not make the situation worse.

10. Teach and reinforce positive morals and values about how others should be treated with respect and dignity.

Sameer Hinduja, Ph.D. is an Associate Professor at Florida Atlantic University and Justin W. Patchin, Ph.D. is an Associate Professor at the University of Wisconsin-Eau Claire. Together, they lecture across the United States on the causes and consequences of cyberbullying and offer comprehensive workshops for parents, teachers, counselors, mental health professionals, law enforcement, youth and others concerned with addressing and preventing online aggression.

Preventing Cyberbullying

Top Ten Tips for Teens

Sameer Hinduja, Ph.D. and Justin W. Patchin, Ph.D.

January 2012

1. Educate yourself

To prevent cyberbullying from occurring you must understand exactly what it is. Research what constitutes cyberbullying, as well as how and where it is most likely to occur. Talk to your friends about what they are seeing and experiencing.

2. Protect your password

Safeguard your password and other private information from prying eyes. Never leave passwords or other identifying information where others can see it. Also, never give out this information to anyone, even your best friend. If others know it, take the time to change it now!

3. Keep photos "PG"

Before posting or sending that sexy image of yourself, consider if it's something you would want your parents, grandparents, and the rest of the world to see. Bullies can use this picture as ammunition to make life miserable for you.

4. Never open unidentified or unsolicited messages

Never open messages (emails, text messages, Facebook messages, etc.) from people you don't know, or from known bullies. Delete them without reading. They could contain viruses that automatically infect your device if opened. Also never click on links to pages that are sent from someone you don't know. These too could contain a virus designed to collect your personal or private information.

5. Log out of online accounts

Don't save passwords in form fields within web sites or your web browser for convenience, and don't stay logged in when you walk away from the computer or cell phone. Don't give anyone even the slightest chance to pose as you online through your device. If you forget to log out of Facebook when using the computer at the library, the next person who uses that computer could get into your account and cause significant problems for you.

6. Pause before you post

Do not post anything that may compromise your reputation. People will judge you based on how you appear to them online. They will also give or deny you opportunities (jobs, scholarships, internships) based on this.

7. Raise awareness

Start a movement, create a club, build a campaign, or host an event to bring awareness to cyberbullying. While you may understand what it is, it's not until others are aware of it too that we can truly prevent it from occurring.

8. Setup privacy controls

Restrict access of your online profile to trusted friends only. Most social networking sites like Facebook and Google + offer you the ability to share certain information with friends only, but these settings must be configured in ordered to ensure maximum protection.

9. "Google" yourself

Regularly search your name in every major search engine (e.g., Google, Bing, Yahoo). If any personal information or photo comes up which may be used by cyberbullies to target you, take action to have it removed before it becomes a problem.

10. Don't be a cyberbully yourself

Treat others how you would want to be treated. By being a jerk to others online, you are reinforcing the idea that the behavior is acceptable.

Sameer Hinduja, Ph.D. is an Associate Professor at Florida Atlantic University and Justin W. Patchin, Ph.D. is an Associate Professor at the University of Wisconsin-Eau Claire. Together, they lecture across the United States and abroad on the causes and consequences of cyberbullying and offer comprehensive workshops for parents, teachers, counselors, mental health professionals, law enforcement, youth and others concerned with addressing and preventing online aggression. The Cyberbullying Research Center is dedicated to providing up-to-date information about the nature, extent, causes, and consequences of cyberbullying among adolescents.

For more information, visit http://www.cyberbullying.us.