Australian Government

acma
Australian Communications and Media Authority

cyber(smart:)

Cybersmart Guide for Families

© Commonwealth of Australia 2009
All rights are reserved.

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be produced by any process without prior written permission from the Australian Communications and Media Authority. Requests and enquiries concerning reproduction and rights, and any enquiries arising from the contents of this booklet, should be addressed to:

Manager Communications and Publishing
Australian Communications and Media Authority
PO Box 13112 Law Courts
Melbourne Vic 8010
Telephone: 03 9963 6800
Facsimile: 03 9963 6899
Email: cybersafety@acma.gov.au

www.cybersmart.gov.au

Introduction

The internet has become an integral part of life. It is a powerful resource, enabling people of all ages to learn and communicate in a myriad of new ways. For children, growing up in a world where the internet has always been available, it is an essential tool. They are the 'digital natives'—always surrounded by online technology, and using the internet from an increasingly early age.

Children can use the internet for many reasons. These could include to:

» find assistance with school assignments
» learn skills
» gain knowledge
» meet new people who share similar interests and
» keep in touch with friends.

But there are risks. Knowing how to use the internet safely is essential to having a positive online experience. For parents and their children, it is important to know how to apply these skills at home, at school and in public places such as the library and internet cafés.

This *Cybersmart Guide for Families* is produced by the Australian Communications and Media Authority (the ACMA) and is part of the Australian Government's broad cybersafety program. The program includes education and awareness activities and resources for parents, children, teachers and library staff throughout Australia.

The ACMA is responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications.

The ACMA's responsibilities include:

» promoting self-regulation and competition in the communications industry, while protecting consumers and other users
» fostering an environment in which electronic media respect community standards and respond to audience and user needs
» managing access to the radiofrequency spectrum
» representing Australia's communications interests internationally.

This guide aims to provide practical advice and information on safe internet use in the home and in public spaces, such as at the library or internet cafes. In learning and applying safe internet skills, and sharing these with their children, parents can help to keep them safe, and ensure that the whole family enjoys positive internet experiences.

The area of internet safety and security is broad, and only key issues are covered in this guide.

For more information or specific advice visit the Cybersmart website www.cybersmart.gov.au or contact the ACMA's Cybersafety Contact Centre on 1800 880 176.

Children's internet activity

The internet is an incredible tool. It offers the chance to become part of an enormous virtual community connected by mutual interest rather than geography. The internet can provide young and old users benefits, including:

» independent learning and research skills and
» improved communication skills, through experience with learning technologies to access and create resources, and communicate with others.

Children access the internet for entertainment, research, school assignments and to communicate. In doing so they can also, often unknowingly, place themselves in risky situations. This includes by:

» giving out personal details about themselves to people or organisations they don't know
» posting unsuitable information online
» agreeing to meet people they've only ever met online, without speaking to a parent or carer
» using provocative pseudonyms
» sharing passwords
» posting public profiles about themselves
» unsafe browsing or searching
» opening messages from people they don't know
» responding to unpleasant or suggestive messages
» using online games or virtual worlds for people over 18 only
» accessing inappropriate or illegal material.

Not all internet users will experience problems. However, ensuring children understand these risks and have the knowledge to be cybersafe is important when accessing the internet at home, at school and in public places.

Specific issues:

Exposure to inappropriate content

Children using the internet can be exposed to content that is inappropriate for them. This could be images, text or games that are sexually explicit or offensive, violent or encourage activities that are dangerous or illegal. Some websites promote extreme political, violent, racist or sexist views. This content can be accessed through website browsing, through newsgroups, shared in peer-to-peer networks or sent by email or instant messaging services.

Young internet users can access inappropriate material inadvertently, when searching for content about people, places or issues. Sometimes, it may be intentional.

Advice for parents

The ACMA administers the Online Content Co-regulatory Scheme, established under Schedules 5 and 7 of the *Broadcasting Services Act 1992*. Parents can complain directly to the ACMA about online content they believe is prohibited by law, by completing an online complaint form available on the ACMA website www.acma.gov.au/hotline.

The ACMA can take action about internet content that falls within the classification RC (refused classification) or X18+. This includes content that contains:

» detailed instruction in crime, violence or drug use
» child pornography
» bestiality
» excessive violence or sexual violence
» material that advocates the doing of a terrorist act
» actual sexual activity.

The ACMA can also take action about content that falls within the R18+ and MA15 + classifications if it is hosted in, or provided from, Australia and is available to minors. This includes content that contains implied sexual activity, strong violence and other material that requires an adult perspective.

The ACMA can investigate complaints made about:

» content on the world wide web
» postings on newsgroups and bulletin boards
» files accessible using peer-to-peer software
» content available on mobile phones.

If the content is prohibited and is hosted in or provided from Australia, the ACMA will direct the provider of the content to remove or restrict access to the content concerned. If internet content that falls within a prohibited classification is hosted outside Australia, the ACMA will notify the content to suppliers of approved filters for blocking. Approved filters are updated regularly.

If the content is sufficiently serious, for example, illegal material such as child pornography, the ACMA will refer the content to the appropriate law enforcement agency for criminal investigation. For more information on the ACMA's role in regulating online content go to www.acma.gov.au/hotline.

Parents can:

» visit the Cybersmart website for internet safety information at www.cybersmart.gov.au
» telephone the Cybersafety Contact Centre on 1800 880 176 for more information or advice
» report to the ACMA any material suspected of being prohibited
» in libraries, ask library staff for information on safe searching techniques, child-friendly websites or how to deal with inappropriate material
» learn more about the internet by attending an internet training session. Ask if these are offered by your local public library.

Cyberbullying

Children using the internet can be cyberbullied or harassed through internet services like email, chat rooms, instant messaging, social networks or through websites. Bullying through mobile phone technologies such as SMS is also considered cyberbullying.

Advice for parents

Cyberbullying includes teasing, spreading online rumours and sending unwanted or threatening messages or defamatory material. While it can have a damaging effect on children and young people, parents can encourage them to take control of the situation. This may be done by:

- advising children not to reply to any messages from a bully. Often if bullies don't receive a response they will give up
- learning how to block a bully, so they can't make contact
- keeping a record of the harassing messages and any replies. This may help parents, or the authorities, if necessary, to find out who is sending them
- keeping usernames and passwords secret. If someone misuses a username and password to post damaging information about a child it can be difficult to remove
- children recognising that if messages are threatening, a parent or carer should be told immediately. Cyberbullying, if threatening, is illegal and can be reported to the police
- contacting the website administrator (often known as the webmaster) to ask for content to be removed, if bullying information has been posted on that website.

Parents can:

- check the privacy settings for your internet services
- visit the Cybersmart website for cyberbullying information
- use support services such as the Kids Helpline or the Bullying No Way website
- talk to the child's school if cyberbullying involves another student
- report threatening messages to the police
- contact the Cybersafety Contact Centre on 1800 880 176 for advice.

Privacy

Without considering the consequences, children sometimes post private information about themselves online. This can include their name or address, photographs, a mobile phone number, their school name and details of their friends or families.

Providing personal information online can also result in being targeted for spam, advertising material and/or viruses. In some cases, websites prompt users to reveal private information on forms or through pop-ups. Not all these requests are legitimate.

Advice for parents

To help guard privacy, children should be encouraged to ask a parent or carer before they give anyone on the internet their personal details. Once information is posted online it is very difficult to remove.

Parents can:

- contact the author or the web administrator if a website contains personal details that have been disclosed without authorisation or their children's personal details. Web administrator details are commonly located on website home pages. A lawyer may also be able to provide assistance
- contact the Office of the Federal Privacy Commissioner if personal details have been mishandled by a Commonwealth Government agency, or a private sector organisation in Australia
- contact the Cybersafety Contact Centre for advice.

Spam

Any library user, including children with a personal email address or mobile phone, can receive unwanted messages. These are called spam. Spam messages may be inappropriate, offensive or contain computer viruses. They frequently promote products or services, but can simply be a message claiming to be from a 'secret admirer or friend'. Responding to these messages can lead to further spam, often at considerable cost to the user if the spam is sent via a mobile phone. Simple safety rules apply—if the message is from someone you don't know, don't click on any link in the email and don't respond in any way.

Advice for parents

Under the *Spam Act 2003* it is illegal to send, or cause to be sent, unsolicited commercial electronic messages. The Act covers email, instant messaging, SMS and MMS—text and image-based mobile phone messaging—of a commercial nature. It does not cover faxes, internet pop-ups or voice telemarketing.

While the Act relates to commercial messages, a message may not necessarily appear to be commercial. Some messages claim to come from a 'secret admirer or friend' but if the recipient fills in their mobile telephone number, they are then sent high-cost premium mobile messages.

Spam complaints should be directed to the ACMA. Action can be taken against spam sent from within Australia. To make a complaint, complete the online form on the ACMA website.

The ACMA has a number of tools available to report spam including the SpamMATTERS reporting button which home users can download.

To download and use SpamMATTERS go to www.acma.gov.au/spam. The ACMA also provides an extensive frequently asked questions section about spam on this site, including advice on how to secure your computer.

Parents can:

- » visit the ACMA website for advice on dealing with spam at www.acma.gov.au/spam
- » report any suspected spam to the ACMA
- » download the SpamMATTERS reporting button
- » contact the Cybersafety Contact Centre for advice.

Unreliable information and scams

Unreliable information

The internet is a valuable research tool for children, providing a wide range of useful information. Children may not realise, however, that information on some websites misrepresents the truth, is misleading, out of date, biased or simply incorrect. For example, websites with racist material may claim to tell the truth about complex social, cultural or historical issues in a way that appears logical and plausible, but isn't.

Advice for parents

Children need to be able to distinguish fact from fiction online and learn the basics about copyright. They also need to develop good browsing and searching skills to ensure they visit safe sites and find appropriate information.

Parents can:

- » review a website before using it. How old is the information? Who wrote it? Does the website have contact details, a privacy policy or copyright statement? If not, find another website
- » advise children to use several sources of information and compare them
- » advise children to acknowledge sources when quoting or reproducing material found online
- » if in a library, ask library staff for a list of safe websites and search techniques.

Scams

Internet scams play on innocent users. Even for children and young users there are ways to tell scams from legitimate offers—and places to lodge a complaint and seek advice if scammed.

Advice for parents

Scammers use the internet in a number of ways—promoting fraud via email, promoting free offers, or creating fraudulent advertising material that is displayed when searching the internet.

Parents can:

- » learn how to recognise a scam. Watch out for an email from an unrecognised sender or one that doesn't have a valid sender's address or opt-out facility. Also watch for use of pop-ups, websites that don't contain a privacy policy or websites that request up-front payment
- » avoid responding to messages from unrecognised email addresses
- » advise children not to complete online forms unless they have checked first with a parent or carer
- » report online scams to the Australian Competition and Consumer Commission's ScamWatch website
- » contact the Cybersafety Contact Centre for advice.

Social networking

Social networking happens on a variety of services like YouTube, MySpace, Facebook and Twitter. These websites allow users to create profiles, communicate with others and form networks of friends. Users can participate in a range of activities including chatting, sharing information and photos and posting comments in forums, blogs or discussion groups.

Different social networking sites have different purposes, including to:

» create communities of friends—MySpace and Bebo
» create and download video content—YouTube and Google Video
» share still photos—Facebook and Flickr.

Advice for parents

Where inappropriate information appears on a social networking website, users can contact the website administrator to request that the offensive content is removed.

Social networking sites generally have policies about unacceptable content, restricting content that users are allowed to upload. For example, some sites limit false profiles, content containing nudity or which presents violence. Website administrators generally rely on complaints from users in identifying unacceptable content, though this can be difficult to monitor because large quantities of content are posted every day.

Users can complain to the ACMA about offensive or illegal material including text, photographs or videos. The ACMA may take action if the material meets the criteria for prohibited content.

When making a complaint, users should provide the web address and any log-in details. Log-in details, such as a user name and password, are particularly important as many social networking sites offer users the ability to restrict information to friends or affiliated users.

Complaints about content can be made at www.acma.gov.au/hotline.

Parents can:

» set house rules about when children can give out or share personal information such as name, address or mobile number
» advise children to set profiles to private so that only people they want to see it can
» encourage children to think before they put anything online. Information posted online can be there indefinitely
» encourage children to be careful when making new friends online—they might not be who they say they are—and never arrange to meet an online friend unless a trusted adult is with them
» report to the ACMA any material suspected of being prohibited
» report abuse or inappropriate content to the website administrator and show children how to do this
» visit the Cybersmart website for more information on social networking
» contact the Cybersafety Contact Centre for advice.

Communication

Children use a variety of services to communicate online. These include chat rooms, blogs, forums, newsgroups, email, multiplayer games, virtual worlds, social networks and instant messaging. Internet users may be able to chat in real time, express opinions, send files, view others through webcams and publish and share personal information including photographs.

Advice for parents

The internet is a public place. The same precautions about interacting with others in real life apply online. Children can forget that people they meet online may not be who they say they are or may experience cyberbullying when communicating online.

Parents can:

- contact the police if they think a child is in immediate danger from contact made online
- advise children that if someone writes something rude or something that makes them feel uncomfortable, they should not respond, and leave the area immediately
- advise children not to open messages from people they don't know, and to delete them straightaway
- encourage children to remember that online friends are really strangers no matter how long they've known them online. Children should speak to a parent or carer if an online friend asks to meet in real life
- advise children to think twice about accepting new 'buddies' or friends—and only accept people they know
- advise children to use an appropriate online name, not their real name, and not give out private information
- learn how to keep a copy of online conversations. Keeping records is useful if there is a need to report suspicious behaviour
- learn how to block people. Users may not wish to see messages from a particular person or receive private messages from them
- visit the Cybersmart website for more information on communicating safely online
- report abuse to the website administrator. Many social networks, virtual networks and gaming sites have these facilities
- contact the Cybersafety Contact Centre for advice.

Using the internet safely at home

Internet safety important is equally important in the home, the library and other public places. By planning to be cybersafe in any location, children are most likely to enjoy fun and rewarding online experiences.

There are four key steps to cybersafe practices in the home:

» **educate**
» **empower**
» **make the computer safe**
» **supervise.**

The four work together towards positive and safe online use. The aim is not only to protect children but to help them learn to make good decisions.

Educate—an essential part of keeping children safe is making them aware of risks, and talking to them about how to avoid potential problems. Visit the Cybersmart website for internet safety information and educational programs suitable for children's use.

Empower—encouraging and supporting children is a positive step towards making them feel confident in their internet use. Children need to know they can make the right choices. They also need to know they can talk to a parent if something happens online that makes them feel uncomfortable.

Make the computer safe—one of the most practical ways to help children stay safe online is to set up the home computer with an internet content filter and other security software.

Supervise—children may behave differently online, to in person, so it's important to be involved. By placing the computer in a family area, supervision becomes easier.

Before starting:

» talk with the family about the importance of staying safe online and having an internet safety plan
» teach children how to use the internet safely. Use an educational program suitable for the child's age
» learn about the internet and the types of internet services children use. Check with the local public library to see what courses are offered.

Set up correctly:

» determine if your internet service provider can assist with advice for staying safe online. If not, switch to one that can
» look at where the computer is set up. If it is in a bedroom, move it to a public area of the house where it's easier to supervise
» make sure safety software is installed on the computer. This may include an internet content filter and other security software such as anti-virus programs, spyware and adware
» use a safe search engine for all web searches.

Create family guidelines:

» discuss the benefits and risks of going online with children and offer support if they get into trouble
» create an internet safety contract with children, setting house rules for internet use.

When online:

- stay involved in the child's use of the internet and new technologies. Work with them. Set up an account, join the child's 'friends' and see what they are doing. It can be a fun experience for parents too
- help the child set up their profile to make sure that they don't put too much personal information online
- check the privacy settings for internet services and see how to report abuse. Many social networking, virtual networks and gaming sites have facilities to do this
- supervise and monitor the use of the internet, particularly with younger children. If issues arise, address them quickly and know who to report problems to
- above all, keep the lines of communication open. Children need to be confident that they can talk to an adult about what's happening, without being afraid that they're automatically going to get into trouble.

Using the internet safely in public places

Internet access

Internet access is readily available at many libraries, internet cafes, some hotels and through mobile phones.

As an example, many public libraries require parental consent for children to use the internet. Some require a parent or carer to be present, while others simply assume parental permission for users who are under 18 years of age. Libraries do not provide supervision for children of any age. Parents are responsible for ensuring that their children abide by library internet-use policies.

Some libraries use internet content filtering software. Most do not. Internet access terminals are usually located in high traffic locations where they are visible to library staff.

Rules about internet use

Rules about internet use are common in most school and public libraries. Generally, these rules cover unlawful and inappropriate use, copyright and other intellectual property rights, access, security, privacy, how to book a session and use of the internet by children. These rules may be in internet-use policies, user behaviour policies or conditions of use statements. Other public spaces offering internet access may also have usage policies. Check with them before going online.

Information and education

While many public internet access points don't provide education materials, libraries are an important source of community information and education on effective and safe internet use. Some libraries provide education, internet training, guides to searching the internet, safe sites for children to visit and trained staff to assist library users.

Many public libraries also provide websites for children that link to resources tailored to their age and interests.

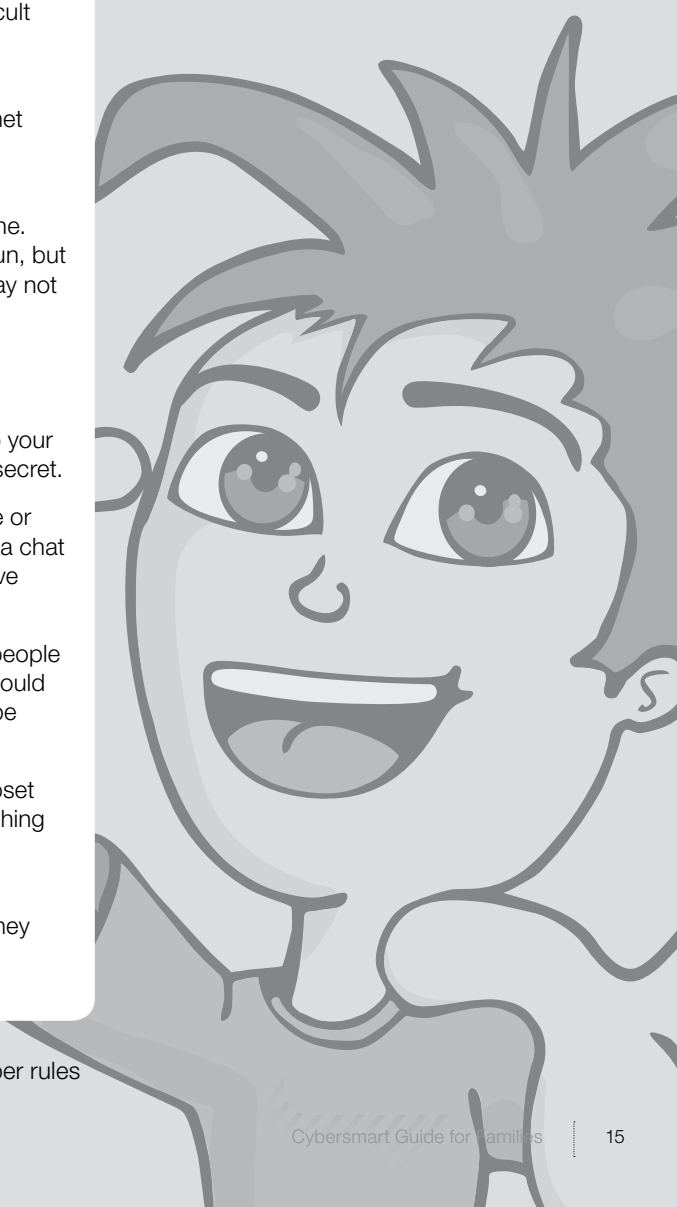
Parents can:

- supervise children when they are using the internet. The level of supervision will depend on the child's age and knowledge
- teach children about the cybersafety rules for internet use. Empowered and informed internet users stay safe and have fun
- educate children about the risks of internet use and safe behaviour. Visit the Cybersmart website for age-specific internet safety information
- become familiar with the conditions of internet use in their local library and communicate these to their children
- find out about the internet. The local public library may run internet training classes
- contact the Cybersafety Contact Centre for advice.

Cyber rules for safe and fun internet use

Young internet users should know how to stay safe and have fun using the internet. One important step is learning the following cybersafety rules:

- Think before you post information online—once posted it's difficult to remove.
- Ask your parent/carer before you give anyone on the internet your name, address or any personal details.
- Be careful who you trust online. Making new friends can be fun, but there's a chance that they may not be who they say they are.
- Always keep your password a secret.
- Set your profile to 'private' so your personal information is kept secret.
- If someone is nasty, offensive or makes you uncomfortable in a chat room, don't respond and leave straightaway.
- Don't open messages from people that you don't know. These could be nasty, contain viruses or be trying to sell you something.
- Tell your parents if you are upset by language, pictures or anything scary on the internet.
- Don't accept any offers that seem too good to be true—they probably are.



For more information about the cyber rules go to www.cybersmart.gov.au

Contacts

Practical solutions

Australian Communications and Media Authority
For information and advice about online safety issues and to order cybersafety resources

Cybersafety Contact Centre
Tel: 1800 880 176
Visit: www.cybersmart.gov.au

To make a complaint about prohibited online content
Visit: www.acma.gov.au/hotline

Bullying No Way
Visit: www.bullyingnoway.com.au

Federal Privacy Commissioner
Tel: 1300 363 992
Visit: www.privacy.gov.au

ScamWatch
Tel: 1300 302 502
Visit: www.scamwatch.gov.au

The Department of Broadband, Communications and the Digital Economy
Advice about online security issues
Visit: www.dbcde.gov.au
Visit: www.staysmartonline.gov.au

Internet Industry Association Security Portal
Further advice about online security issues
Tel: 02 6232 6900
Email: info@iia.net.au
Visit: www.security.iia.net.au

Report a crime

Crime Stoppers
Tel: 1800 333 000

AFP High Tech Crime Operations
Further advice and to report electronic crime
Visit: www.afp.gov.au

AFP Child Protection Operations Team
Report concerns about inappropriate online behaviour towards children
Visit: www.afp.gov.au/online_form/ocset_form.html

Talk to someone

Reach Out
Visit: www.reachout.com.au
Email: info@reachout.com.au

Life Line
Tel: 13 11 14
Visit: www.lifeline.com.au

Kids Helpline
Tel: 1800 55 1800
Visit: www.kidshelp.com.au

Australian Communications and Media Authority
Cybersafety Contact Centre
For advice about online safety issues
and to order cybersafety resources
Tel: 1800 880 176
Visit: www.cybersmart.gov.au
Email: cybersafety@acma.gov.au

Canberra Office
Purple Building, Benjamin Offices
Chan Street, Belconnen
PO Box 78,
Belconnen ACT 2616

Tel: 02 6219 5555
Fax: 02 6219 5200

Melbourne Office
Level 44, Melbourne Central Tower
360 Elizabeth Street, Melbourne
PO Box 13112 Law Courts
Melbourne Vic 8010

Tel: 03 9963 6800
Fax: 03 9963 6899
TTY: 03 9963 6948

Sydney Office
Level 15, Tower 1 Darling Park
201 Sussex Street, Sydney
PO Box Q500
Queen Victoria Building NSW 1230

Tel: 02 9334 7700, 1800 226 667
Fax: 02 9334 7799