A parent's guide to internet safety

HOW TO KEEP YOUNG INTERNET USERS SAFE

Contents

Introduction

NetAlert is the Australian Government's online safety program, set up to protect Australian families online. NetAlert is part of the Australian Communications and Media Authority (ACMA).

NetAlert provides practical advice on internet safety, parental control and filters for the protection of children, students and families. It offers information on the issues, risks and dangers associated with using the internet, and advice on how to minimise risks, avoid problems and use the internet safely and responsibly. NetAlert works closely with other government and state agencies, the internet industry and community organisations to promote internet safety.

NetAlert can show you how to make the internet safer for your family. Its primary objective is promoting a safer internet experience. NetAlert provides advice on a whole range of internet safety options—free guidance, information and resources designed to help you develop your own family safety strategy.

This guide provides parents and carers with advice, information and the tools to keep children safe when using the internet, as well as empowering children who use the internet. It considers what children are doing on the internet according to their age, the dangers associated with using the internet and the strategies parents and carers can use to minimise risks.

Internet safety checklist

This checklist provides a summary of the key things you should know to keep your family safe when using the internet.

BEFORE YOU START

- Talk to your family about the importance of staying safe online and the need to have an internet safety plan for your home.

- Teach your children how to use the internet safely. NetAlert has a range of free educational programs for different age groups.

GETTING SET UP CORRECTLY

- Check if you are connected to a family-friendly internet service provider. If not, switch to one that can help you with internet safety.

- Look at where the computer is set up at home. It should be in a public area of the house, not in a bedroom, where it will be easier for you to supervise.

- Make sure you have safety software installed on your computer. This may include a filter and other security software such as anti-virus programs, spyware and ad-aware. NetAlert can give you advice on what to get.

- Use a family-friendly search engine for all web searches.

CREATE FAMILY GUIDELINES

- Discuss the benefits and risks of going online with your children and reassure them that you are there to help if they get into trouble.

- Create an internet safety contract with your children and set up house rules for use of the internet. NetAlert has samples to help you.

WHEN ONLINE

- Supervise and monitor the use of the internet with your family. If issues arise address them quickly and know who to report problems to.

- Encourage and support your family with their use of the internet. Teach them to make right decisions and increase the levels of responsibility as children get older.

Understanding the internet

WHAT IS THE INTERNET?

The internet is a global network of linked computers that are able to communicate through telephone lines, cables and satellites. Connecting to the internet enables you to transmit and share information in the form of text, pictures, movies and sound. Anybody can connect to the internet if they have an internet-ready computer and an account with an internet service provider.

There is no central 'home' for the internet. It has been designed to operate from many different locations. No organisation or individual owns the internet, but countries can legislate regarding usage or content.

WHAT SERVICES ARE AVAILABLE ON THE INTERNET?

Once connected to the internet you can access a variety of activities called internet services. Internet services change as technology advances. New ways to use the internet are being discovered on a regular basis. Current popular internet services include:

- Web browsing— – using an internet browser program to search and view web pages. Web pages can include text, pictures, sound and video.

- Email—a service that lets you send a written message to another person via the internet. The message is stored on a computer and is read when the recipient checks their mail – just like checking your real mailbox. People using email require an email address, which identifies them as a unique person online. Internet service providers supply email addresses to people when they open an internet account. You can also attach and send a variety of files to accompany your message.

- Chat—used to send instant messages to other people on the internet. Messages can be sent to friends or strangers. Chat rooms are online meeting places where people congregate to send messages back and forth to each other.

- Newsgroups—places on the internet where people can post messages about a topic. People with similar interests will read the message and post replies. Newsgroups can either be moderated (where each message is checked over before it is placed on the internet) or public (where messages are posted automatically).

Children and the internet

Today, children are exposed to the internet at an early age and from a variety of places. These include:

- school—computers can be found in all levels of the education system;

- home—many homes now have personal computers with internet access;

- friends—if your child does not have access to the internet at home, it is likely that a friend does;

- libraries—public libraries have internet computer terminals for use by patrons;

- public access centres—public places where people can access the internet; and

- mobile internet-enabled devices—mobile devices such as phones can access the internet.

With so many options available, children can easily access the internet. This is why you need to prepare your children for internet safety, just as you would for other issues such as fire, road and water safety.

Being prepared with an internet safety strategy for your children will reduce the risk of problems occurring.

What are my children doing on the internet?

Many parents feel that their children know more than they do about using the internet. The following sections explore the kinds of things your child may be accessing on the internet.

WHAT ARE CHILDREN AGED 2–7 YEARS DOING ONLINE?

Preschoolers are old enough to begin to explore the internet and to learn about the computer. Children from about five years may start to visit children's websites with you and enjoy email correspondence with family and friends.

NetAlert has a free internet safety educational program available for young children.

Go to www.nettysworld.com.au.

What parents can do
- Check out good sites for younger children—you should be responsible for selecting the sites that children in this age group can visit.

- Very close supervision is strongly recommended.

- Select sites and set up bookmarks for very young users.

- Consider using 'safe zones' for this age group, particularly when they start school and can do more on their own.

- Limit email correspondence to a list of friends and family members you have approved.

- Use filters to limit accidental access to unsuitable material.

WHAT ARE CHILDREN AGED 8–11 DOING ONLINE?

From around eight years old, children become increasingly interested in exploring the internet, chatting and corresponding online. Some older children may begin to assert their independence and look for 'forbidden' material. Marketers may target them, but increasingly they learn to recognise the difference between advertising and other material. It helps to talk to children about commercial information and ways to deal with it. Their skills and independence will continue to increase, but making internet exploration a family activity allows you to maintain close supervision.

NetAlert has created a free internet safety educational program for children aged 8–12 years.

Go to www.cyberquoll.com.au.

What parents can do
- Be actively involved in your child's internet use.

- Emphasise safe online behaviour and discuss why this is needed.

- Investigate any chat rooms or online clubs that your child wants to join to make sure they are legitimate.

- Consider using 'filters' to block access to internet relay chat (IRC) and newsgroups.
- Discuss use of good cyber manners ('netiquette').
- Keep the computer in a public area of the home to supervise children's use.
- Use family-friendly search engines designed for children.

WHAT ARE CHILDREN AGED 12–18 DOING ONLINE?

The internet becomes a valuable tool for homework and projects for teenagers. At the same time, younger teens start to become more independent and self-assured, wanting more freedom and coming under more peer influence. Their online and email contacts tend to expand. Some may challenge the use of filtering software and attempt to access 'forbidden' material. Many are 'net savvy'—they know about hacking into systems and understand basic computer programming. However, they are more able to differentiate between advertisements and other material, and recognise persuasion techniques.

Many older teens can write their own programs and know how to manage computer hardware and software. Their use of the internet includes school research, job and further education searches, global communication and enhancing their technical skills. This increasing knowledge can also get them into trouble if they explore ways of getting around technical tools and methods for breaking into private systems.

What parents can do
- Stay in touch with what your children are doing online. While it may become less feasible to actively supervise their access, continue to discuss internet issues and share internet experiences.
- Keep the computer in a public area of the home.
- Reinforce safety messages and cyber rules. NetAlert has created house rules and internet safety contracts to help families create internet safety strategies. Younger teens in particular should be reminded of the need to protect their privacy.
- Ensure that teens understand that posting to newsgroups makes their email address public.
- Ensure that both you and your teenager understand laws relating to copyright, privacy, software piracy, hacking and obscenity.

Despite the educational and social benefits of the internet, there are risks associated with its use.

Children and adolescents accessing the internet may be confronted with material that is disturbing or inappropriate. Although there are technological measures than can be adopted to minimise the risks, other strategies include educating children as early as possible about the benefits and dangers of using the internet. It is essential to instruct children about how to be 'street-smart' and to use the internet in a safe and responsible manner.

Some potential dangers for children

EXPOSURE TO INAPPROPRIATE MATERIAL

There is a risk that children may be exposed to material that is pornographic, sexually explicit or offensive, hateful or violent in nature, or that encourages activities that are dangerous or illegal.

Some sites promote extreme political, violent, racist or sexist views. Such materials can be accessed via the World Wide Web or newsgroups, shared in peer-to-peer (P2P) networks, or sent via email or instant messaging services.

Access to such material may occur inadvertently through searching for educational content about people, places or issues. Children should be aware of safe searching techniques and use a family-friendly search engine for searches. Parents should be aware of who to report problems to and how to deal with unsolicited inappropriate material.

PHYSICAL DANGER

'Stranger danger' is also a risk associated with the internet. It is possible your child may physically meet a person who may claim online to be someone they are not. It is vital that children know not to provide personal information to anyone they meet online. In some cases paedophiles have used chat rooms, email and instant messages to gain a child's confidence, and then arrange a face-to-face meeting.

UNWANTED ADVERTISING AND MARKETING TOWARDS CHILDREN

Commercialisation of the internet is on the increase. This high level of commercialism is evident in World Wide Web, in email, in online marketing – even taking the form of online gambling.

Scam websites have been set up to deprive people of money or opportunity. Some websites may be bogus or dummy sites—for example, websites supposedly belonging to banks which have been developed to deceive people into providing credit card details (known as 'phishing'). Because of the persuasive nature of these bogus sites, children may put themselves or their family at financial risk by providing their own or their parents' credit card details. The basic rule of thumb is that if something seems too good to be true, it probably is!

FINANCIAL RISKS

Another financial risk related to internet use is called 'dumping'. Internet dumping occurs when somebody is tricked into disconnecting from the internet at the normal cheaper rate and unknowingly reconnecting at a more expensive rate. It often occurs when you click on a web page element, such as a picture or link, which contains a malicious computer code.

The expensive rates are usually an international or premium number, such as the 190, 191, 192 prefix numbers. These numbers are often timed, so the longer you stay connected, the more expensive the account will be. If a large sum of money appears mysteriously on your telephone bill, you may have been a victim of an internet dumping scam.

HARASSMENT AND BULLYING

Cyber bullying can be carried out through internet services such as email, chat rooms, discussion groups, instant messaging or web pages. It can also include bullying through mobile phone technologies such as SMS. Cyber bullying can include teasing and being made fun of, spreading rumours online, sending unwanted messages and defamation.

EXPLOITATION

Some websites prompt people to complete a form revealing their name, email address, age and gender, and sometimes even their telephone number and postal address, in order to access information. Some requests are legitimate – much depends on the nature of the website requesting the information. Providing personal information online can result in a person being targeted for spam (unsolicited email), advertising materials and/or viruses. Privacy issues also apply to developing personal websites and publishing online. Providing personal details,

including photographs, may lead to the information being captured and reused by others for illicit purposes.

PERSONAL INFORMATION AND PRIVACY

Just as you would not provide personal information to someone you meet on the street, neither should you do so on the internet. Issues to do with identity protection revolve mainly around web authoring and website requests for such information. Creating web pages can be a fun and educational experience for children. However, there is a danger that children will post home addresses and other personal details on websites, including photographs of themselves or other children. This carries the risk of such material being used inappropriately. Likewise, placing a child's email address on a website could lead to them receiving sexually explicit or offensive emails.

UNRELIABLE INFORMATION

Information on some websites may misrepresent the truth, be misleading, be out of date, biased or just incorrect. Some racist websites claim to tell or represent the truth about complex social, cultural or historical issues in ways that appear logical and plausible. Such websites are known to actively merchandise or even recruit people.

SPAM

Spam is the email equivalent of junk mail or nuisance telephone calls. Spam is simply any unsolicited electronic mail sent in bulk to individuals or organisations. It can include viruses or pornographic content. Spam is becoming increasingly prevalent and is an issue for anyone with a personal email address. Filters can be used to prevent spam from entering a mailbox, but spammers are using increasingly sophisticated techniques to bypass filters. Children need to recognise and delete spam without opening it.

VIRUSES

While email is a useful way of communicating and sharing information, risks include unsolicited email from unknown senders that may contain virus-infected attachments or links that lead to a virus-infected website.

COMMUNICATION

Internet technologies such as email, chat rooms and electronic conferencing are fast, easy and effective means of communicating and sharing information. internet-enabled devices including mobile and camera phones and personal digital assistant (PDAs) can also be used for text messaging and exchanging photographs or video. There are, however, some risks associated with using these technologies:

There are, however, some risks associated with using these technologies:

- Emails can contain virus-infected attachments or be used to bully and harass, including of sexual harassment or racial vilification.

- Text messages can be used for the same purpose.

- In chat rooms the same risks apply, and in unmoderated chat room environments people may adopt false identities. This is known as 'online grooming'.

- In extreme cases, students can be exposed to physical danger in the event of a face-to-face meeting with someone they may have met in a chat room.

The internet offers an enormous range of opportunities for your family. Instant communication, information discovery and online publishing open up a world of exploration and fun for children of all ages. However, as in the real world, there are potential problems and risks associated with internet use. By adopting an internet safety strategy, your children can be protected online. There are four basic ways you can achieve this:

- education;

- encouragement and support;

- make the computer safe; and

- supervision.

Using all four ways together will give you the best results. The aim is not only to protect children, but to help them learn to make the right decisions when faced with a dangerous situation online.

Educate your children on internet safety

An essential part of keeping your children safe is to make them aware of the dangers, and to talk to them about how to avoid potential problems. NetAlert has a range of educational programs available free of charge, developed to teach children important internet safety skills.

PARENT'S INTERNET SAFETY TOOLKIT

An internet safety educational program created by and for parents. Learn about the issues and what you can do to keep your children safe using the internet. The program is available free from NetAlert on CD-rom and comes with an accompanying explanatory booklet, or access the toolkit online from www.netalert.gov.au.

FREE INTERNET SAFETY KIT

NetAlert's free internet safety kit contains *A parent's guide to internet safety*, as well as many other useful materials to help you educate your children on internet safety. There is information in the kit that gives general help and advice for children of all ages. Contact NetAlert on 1800 880 176 or email netalert@acma.gov.au to find out more about the kit or to order your free kit.

NETTY'S WORLD

Netty's World is designed for young children starting out on the internet. It provides an interactive and safe play environment for children, with important messages about internet safety.

NetAlert encourages parents to take their children through the online storybook, *Netty's Net Adventure*, which explains important internet safety messages. Following this, children are encouraged to play the interactive games where the internet safety messages are reinforced.

Go to *Netty's World* at www.nettysworld.com.au.

CYBERSAFE SCHOOLS

CyberSafe Schools is an education program that has been designed for schools but can also be used by parents in the home. There are three areas in the CyberSafe Schools program:

- guides for educators;

- resources for younger children (primary age); and

- resources for older children (secondary age).

New resources will be continually developed for this program, so keep an eye out for something you can use in the home.

Go to www.netalert.gov.au.

CYBERQUOLL

CyberQuoll is an internet safety interactive educational program for primary school children aged 8 to 12 years.

Go to www.cyberquoll.com.au.

Empower your children

Encouraging and supporting your children is a very positive step towards making them feel confident in their use of the internet. Remember that children will have access to the internet not only in the home, but also at other places they go to such as schools, friends' houses and libraries.

By allowing them to make informed decisions about the content they access, and by developing a sense of trust at home, your children will be in a good position to use the internet in a responsible way when they are away from home.

MAKE YOUR COMPUTER SAFE

One of the most practical ways to help your children stay safe online is to set up your home computer for safe use.

Safety software

NetAlert recommends that you install a filter on your computer to protect your family from unwanted content and to help manage your children's internet access. Filters often form part of readily available safety software packages.

It is a good idea to ask your computer retailer what safety and security software comes with your computer, or what is missing.

Programs
- Internet filters can block out or permit access to certain types of content on the internet.
- Install security software like virus, firewall and spyware protection to help with security and privacy.
- Spam filters block out unwanted junk email—current versions of email programs such as 'Outlook' now have spam filters built in.
- Parental monitoring software can help you monitor what your children are doing online. They can also often block access to specific programs.
- Pop-up stoppers stop new windows from popping up on your screen.

Other things you can do
- Enable internet browser security—change the settings in your internet browser to ensure your computer can recognise sites which may be labelled as inappropriate.
- Monitor your programs—remove any programs that are not needed and check for any new ones that may be installed by children.
- Check history—check the history folders on your computer to view what sites have been accessed.

- Update software—make sure that all the programs you have installed are up-to-date. New versions of programs are often released.

- Filters—can block a user's access to websites and specific internet services.

Many of the safety programs we suggest you use are available from your internet service provider, retailer or by downloading them from the internet. There are a number of packages available that can perform many of the things you need, so purchasing one of those may be the easiest thing to do.

You may wish to have a look at some particular programs we recommend. These are especially suited for use in the home.

Family-friendly internet service providers

Be sure to choose the right internet service provider. The Internet Industry Association has developed a 'ladybird seal' for internet service providers who demonstrate best practice standards. Look for this symbol when choosing your service provider.

Supervise your children's internet use

At home, the best protection for a child using the internet is parental supervision and guidance.

You would not let your children rent out an X-rated video, so why risk the possibility of your children being exposed to X-rated content on the internet?

By placing your computer in a family area, supervision becomes easier than if it is in your child's bedroom.

THE WORLD WIDE WEB

Visiting websites is the most common activity undertaken on the internet. Children and adolescents accessing the internet using a computer or other enabled devices may be confronted with material that is disturbing or inappropriate. The Australian Government and the Australian States and Territories have responded to this with a number of initiatives, including state-wide wide area networks (WANs), filtering services and moderated search engines.

EMAIL

Email (electronic mail) is a message that can be sent over the internet to someone else. It is one of the services provided by an internet service provider (ISP). It is like sending a letter or a postcard to anywhere in the world instantly. Documents, images, text, music and movies can be attached to emails. The risks with email include spam or spamming, 'flaming', 'bombing', stalking, viruses, bullying and inappropriate content.

CHATTING

'Chatting' is a way of communicating with people by typing messages which are sent across the internet to be read by others participating in the chat room – a virtual meeting place. The process of taking part is known as 'chatting'. Participants are sometimes known as 'chatters'. Chat rooms have an element of anonymity about them, so children and adolescents often talk about things they may not have the confidence to say face-to-face. They can pretend to be someone else—older, smarter or more popular. The anonymity of participants may lead children to engage in unsafe behaviour or to become susceptible to cyber stalkers who can skilfully imitate a young person's 'voice'. Children need to be careful about how much personal information they give out when chatting.

INSTANT MESSAGING

Instant messaging is a form of online chat involving two or more individuals. When you send an instant message to someone it appears on their screen almost instantly. Some services also allow the sending of files to one another. Internet messaging is also called IM, Iming, internet relay Chat (IRC), or ICQ ('I seek you'). Using instant messaging programs exposes children to a number of risks. Private conversations are easy to start with anybody and real time conversations can occur with strangers. As a result, personal information may be inadvertently released.

PEER-TO-PEER (P2P) NETWORKING

P2P networking programs are applications that run on personal computers with the intent of sharing files with users across the internet. P2P networks work by connecting individual computers and forming filesharing communities. Members of the community can then search for files or share files with the rest of the community. When a search is conducted, all the available computers that are sharing files in the community are requested for the file. If found, the user can start downloading it.

Common uses for P2P networking include sharing music, pictures, movie files and other documents. Risks associated with this technology can be exposure to inappropriate content, downloading of viruses or spyware, or breaching copyright regulations for protected works. Often, files that are downloaded are not what they say they are in the filename or file description.

WEB AUTHORING

Many children develop websites for school projects or for personal interest. It is essential that they protect their identities by not publishing detailed personal information, names, email addresses or photographs.

MOBILE INTERNET-ENABLED TECHNOLOGIES

Today there is a range of mobile internet enabled devices that let you access the internet using a wireless connection on a portable device. Such devices can include mobile phones, personal digital assistants (PDAs) and palmtops. They connect through a new communications network called, 'third generation wireless' or simply '3G'.

This network allows a range of internet services to be accessed including digital content, rich media, internet access, chat and instant messaging and video streaming. Since the 3G network started in Australia, the take-up of mobile internet-enabled devices, particularly among children, has been dramatic. Mobile devices are becoming more sophisticated and the cost is decreasing, making them more affordable and accessible to children.

As well as this ease of unsupervised access, many devices also have the ability to take digital pictures or play digitised music, making the notion of mobile access to the internet very appealing to children.

The internet is just like any public place where your child can be exposed to danger. These new mobile devices may expose your child to danger virtually anywhere and anytime. For example:

- parents cannot tell when children are using the device, making supervision hard;

- a child has easy access to inappropriate and potentially illegal content;

- a child is exposed to inappropriate contact, including luring and grooming activities;

- children's vulnerability to internet marketing and their loss of privacy;

- children are easier to locate as the mobile is 'always on';
- there is a higher chance of being exposed to internet marketers;
- there is an increased risk of the child either being stalked or bullied by others;
- the risk of identity theft, loss of privacy, stealing and misuse of equipment; and
- possible unexpected high expenses.

Mobile phones and safety

Many parents buy a mobile phone for their child for safety reasons. Knowing that your child is contactable at all times brings enormous peace of mind. However, mobile phones can expose children to a range of risks.

Few parents are aware that newer mobiles can access the internet, potentially exposing their children to unsuitable content. Educating your child on safe mobile phone use is essential, as most children lack the maturity to understand the risks mobile phones can pose.

What are some of the attractions?

Mobile phones have become popular with children for many reasons, including:

- personal—gives children a sense of ownership;
- private—can be used when and where a child likes;
- image and fashion—can portray an image to others;
- constant communication—children enjoy communications;
- price—affordability of certain mobile phone 'plans';
- services—games, SMS, music, video streaming, chat, instant messaging and internet access are all available and accessible to children; and
- features—many mobile phones have multi-functions and can be used as digital cameras, radios or storage devices.

Ten things you can do *now* to help children stay safe

- Understand what a device does before you buy. Don't sign up for services you don't want your children to access. Ask about blocking inappropriate service options.
- Make sure any device you purchase is appropriate to the age and experience of your child.
- Become familiar with the mobile technologies your children use or are introduced to by their friends.
- Don't give your children mobile phones just for the sake of it – inform yourself of all the risks and benefits before making a decision.
- Create a family contract with agreed consequences for exceeding time limits or cost.
- Involve your children in decision-making about internet accounts, mobile phone services and price plans so that they share responsibility for the cost of their activities online.
- Don't use prepaid mobile phone accounts if you need to monitor usage or manage SMS addiction.
- Strangers may be able to access information on your Bluetooth-enabled phone. Set your phone to 'undiscoverable'.
- Use your phone's handset PIN to protect it against unauthorised use. Keep your PIN numbers secret.

- Find and record your phone's IMEI number. This can assist police in recovering a lost or stolen phone.

MAKE YOUR CHILD'S INTERNET EXPERIENCE SAFER

Never	Always
Never tell anyone you meet on the internet your telephone number, home address or your school's name unless your parent/guardian specifically gives you permission.	Always be very careful in chat rooms. Even if a chat room says it is only for children, there is no way to tell if everyone there is really a child. It might be an adult or an older child trying to trick you.
Never send your picture, credit card or bank details to anyone, without first checking with your parent/guardian.	Always check with your parent/guardian that it is okay to be in a chat room.
Never arrange to meet anyone unless your parent/guardian goes with you and you meet in a public place. People you contact online are not always who they seem or who they say they are.	Always leave a chat room if someone says or writes something which makes you feel uncomfortable or worried and make sure you tell your parent/guardian.
Never open attachments to emails unless they come from someone you know and trust. They could contain viruses or other programs which would destroy all the information and software on your computer.	Always keep your password to yourself; do not tell anyone what it is.
Never respond to nasty or suggestive messages and always tell your parent/guardian if you get these.	Always stay away from sites that say they are for people over 18 only. The warnings are there to protect you. Adult sites can sometimes cost a lot more on your phone bill too.
	Always remember if someone makes you an offer that seems too good to be true, it is probably a trick.

About NetAlert

NetAlert is the Australian Government's online safety program, set up to protect Australian families online. NetAlert is part of the Australian Communications and Media Authority (ACMA). NetAlert offers a range of advice, online resources and educational materials free of charge.

Contact NetAlert at:

PO Box 13112 Law Courts
Melbourne Vic 3000
Tel: 1800 880 176
Fax: (03) 9963 6899
www.netalert.gov.au

For information in another language, call 131 450 from anywhere in Australia, for the cost of a local call. The Translating and Interpreting Service can call ACMA on your behalf.

Resources

INTERNET SAFETY CONTACTS

Emergency

When a child is in immediate danger of abuse

Website: www.crimestoppers.com.au

Tel: 000, or Crimestoppers on 1800 005 555

Law Enforcement

Report suspected cases of child abuse or contact with paedophiles

Online Child Sex Exploitation Team (OCSET), a unit of the Australian Federal Police

Website: www.afp.gov.au

Tel: (07) 5553 8717

Email: National-OCSET-OMC@afp.gov.au

Report online criminal activity (e-crime)

Australian High Tech Crime Centre (AHTCC), a unit of the Australian Federal Police

Website: www.afp.gov.au or www.ahtcc.gov.au

Tel: (02) 6256 7777

Report any crime involving children online or online services

Australian Federal Police (AFP)

Website: www.afp.gov.au or www.ahtcc.gov.au

Tel: (02) 6256 7777

Government

Report inappropriate or illegal online content, or problems with a telecommunications service or provider

Australian Communications and Media Authority (ACMA)

Website: www.acma.gov.au

Tel: 1800 226 667

For help and advice about online privacy issues

Office of the Federal Privacy Commissioner Australia

Visit: www.privacy.gov.au

Phone 1300 363 992

Complain about inappropriate content in computer games, video and DVD programs

Office of Film and Literature Classification (OFLC)

Website: www.ofl c.gov.au

Tel: (02) 9289 7100

Consumer complaints about online business practices

Australian Competition and Consumer Commission (ACCC)

Website: www.accc.gov.au

Tel: 1300 302 502

Complain about internet service providers

Telecommunications Industry Ombudsman (TIO)

Website: www.tio.com.au

Tel: 1800 062 058

Report cases of racial hatred or sex discrimination

Human Rights Equal Opportunities Commission (HREOC)

Website: www.humanrights.gov.au

Tel: 1300 656 419

Report cases of online financial scams or fraud involving Australian companies

Australian Securities and Investments Commission (ASIC)

Website: www.asic.gov.au

Tel: (03) 5177 3988

Industry

Technical information on internet security, viruses, firewalls and internet service providers

Internet Industry Association (IIA) Security Portal

Website: www.iia.net.au

Tel: (02) 6232 6900

Complain about 190 telephone information services in Australia

Telephone Information Services Standards Council (TISSC)

Website: www.190complaints.com.au

Tel: 1300 139 955

Community

For information about psychological issues such as internet addiction disorder

Australian Psychological Society (APS)

Website: www.psychology.org.au

Tel: 1800 333 497

Glossary

Attachment

This is a file of information that is sent with an email. It may contain text, photos, graphics, sound or video.

Acceptable user policy

These are documents created by systems or schools to outline what is acceptable behaviour when using computer facilities.

ACMA

The Australian Communications and Media Authority is Australia's regulator for broadcasting, the internet, radiocommunications and telecommunications. You can complain to ACMA about internet content that is, or may be, prohibited by law. There are a number of ways to lodge a complaint. Go to www.acma.gov.au.

Blog

The word blog is derived from the combination of the two words web and log. Blogs are virtual diaries created by individuals and stored on the internet. Blogs generally consist of text and images and can appear in a calendar-type format.

Broadband

Sometimes referred to as a high-speed internet, broadband is an 'always on' fast connection to the internet. Today there are a wide variety of broadband technologies available in most areas; two of the more commonly found and used technologies are cable and DSL broadband.

CD-ROM

CD-ROM stands for 'compact disk – read-only memory'. A compact disk can store large amounts of information and is inserted into a computer's CD-ROM drive.

Chat room

A chat room is a place on the internet where people with similar interests can meet and communicate together by typing messages on their computer. People can often enter an unmoderated chat room without any verification of who they are. Problems for students can arise with chat room participants pretending to be someone they are not.

Cyber bullying

Bullying which is carried out through an internet service such as email, chat room, discussion group or instant messaging. It can also include bullying through mobile phone technologies such as short message services (SMS).

Cyberspace

The online world of computer networks.

Download

By downloading something (like a music file, document or photo) you are transferring information from the internet to your computer.

E-crime

E-crime is where a computer or other electronic communications device, such as a mobile phone, is used to commit an offence, be the target of an offence or act as a storage device in an offence.

Email

Email is a service that lets you send a message, like a letter, to another person via the internet. The message is stored on a computer and is read when the recipient checks their mail – a little like checking your real mailbox.

Emoticons

An emoticon is a word derived from the two words emotions and icons. Emoticons are a shorthand method of explaining a feeling on the internet. Emoticons can be used in any communication over the internet but are particularly popular with chat rooms and instant messaging. Here's an example of an emoticon: :) = happy.

Filter

A filter manages access to online content. A filter can restrict times when the internet can be accessed and also restrict what is viewed and downloaded. Some filters can also be instructed to specifically block information from being displayed, even if children type it in. Types of filters range from home filters to filters used by a school on its server.

Firewall

Firewalls can limit and stop access to computers by unauthorised people or systems. A personal firewall can be installed on your computer to protect it from intruders on the internet. Firewalls can be used to stop the spread of viruses and spam and can be a valuable tool in protecting children online.

Flaming

Flaming is the sending of messages that include bad language or repeat messaging especially of undesirable or obscene text. Flaming (also known as 'flame wars') occurs in unmoderated chat rooms. The majority of chat rooms remain 'open' where messages are posted automatically with no human intervention.

Handle

A handle is a name for a person that is used in the online world. When a person signs up for a service such as Hotmail or ICQ, they are required to create a unique identifier – a 'handle'. When in a chat room you should always use a handle.

Identity theft

Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes. Identity theft is a form of identity crime (where somebody uses a false identity to commit a crime).

Instant messaging

An instant messaging program is one that can instantly send messages from one computer to another by means of small 'pop-up' windows. They are a form of 'instant email' and are very popular with students and adults alike. They are usually a one-to-one communication medium, although some programs allow many people to chat at the same time, like a private chat room.

Internet acronyms

internet acronyms are acronyms that are used specifically on the internet or mobile phones as a method of communication. They are popular because they save people time in preparing messages. It is quicker, for example, to type in one acronym which is easily understood, than a series of words.

Internet content

This encompasses all forms of information including text, pictures, animation, video and sound recording, and may include software.

Mobile internet-enabled devices

Mobile devices such as phones which are able to access the internet, take photographs and sometimes record sound.

Netiquette

Netiquette is derived from the two words internet and etiquette. Netiquette describes 'the rules' for how one should act online especially in newsgroups, forums and chat rooms. Netiquette can also be applied to email creation and transmission.

Newsgroups

Newsgroups are also known as online forums and are places on the internet where people can contribute to a discussion by leaving a message of interest. Newsgroups exist on thousands of topics, and are useful for building online communities and bringing people together with similar interests. Unrestricted or unmoderated newsgroups pose significant safety risks for students.

Password

A password that you use on the internet works in a similar way to a password you may use in real life. Your password should never be given to anyone other than your parents/guardian. You should password-protect all blogs and websites you may create. This will ensure that only people you authorise can access the site.

Peer-to-peer (P2P) networking

P2P is an application that runs on a personal computer and shares files with other users across the internet. P2P networks work by connecting individual computers together to share files instead of having to go through a central server.

Phishing

'Phishing '(also known as 'phising') is the practice whereby a fraudster who is pretending to be from a legitimate organisation sends misleading emails requesting personal and financial details from unsuspecting people.

Pop-ups

Pop-ups are small windows that appear in the foreground of an internet browser. Pop-ups are often used to display advertising or pornography on the screen, however they can be integrated into some websites for practical purposes.

Safe zones

Safe zones are an alternative to filtering or labelling. Labelling allows web developers to categorise online content on the basis of language, violence, sexual content, and so on. Safe zones are services providing access to a range of sites, which are suitable for children.

Spam

Spam is the email equivalent of junk email or nuisance phone calls. Spam can simply be defined as all unsolicited electronic mail sent out in bulk to individuals/organisations that have not consented to receive it.

Spyware

Spyware is a computer program which can be installed on personal computers (usually without the permission from the owner) and has the purpose of collecting information and sending it back to another source, usually an internet marketing or pornographic website.

Stranger danger

This term describes the potential dangers in meeting a stranger online. Adults may pretend to be children in chat rooms or other internet services. It is important for students to realise they may not be communicating to the person they think they are.

Unreliable information

Information on the internet may misrepresent the truth, be out of date, biased or just incorrect.

Unsolicited email

Electronic mail that is unrequested by the recipient and is of an advertising or promotional nature.

URL (address)

URL stands for 'uniform resource locator' which is the address of a file or content on the internet. They begin with www (world wide web), followed by the name of the company or product. For example, the URL for NetAlert is 'www.netalert.gov.au'.

User

A user of the internet.

Virus

A virus is a computer program (usually disguised as something else) which is designed to cause undesirable effects on computer systems. Viruses are often designed so that they can be transferred from one computer to another without the users knowing. They can be hidden in emails, on CDs or in files that are shared across the internet. Computer viruses can cause harm to computer systems and need to be avoided.

Web page

Means a file or content accessible on the World Wide Web by requesting a single URL.

PO Box 13112 Law Courts
Melbourne Vic 3000
Tel: 1800 880 176
Fax: (03) 9963 6899

www.netalert.gov.au