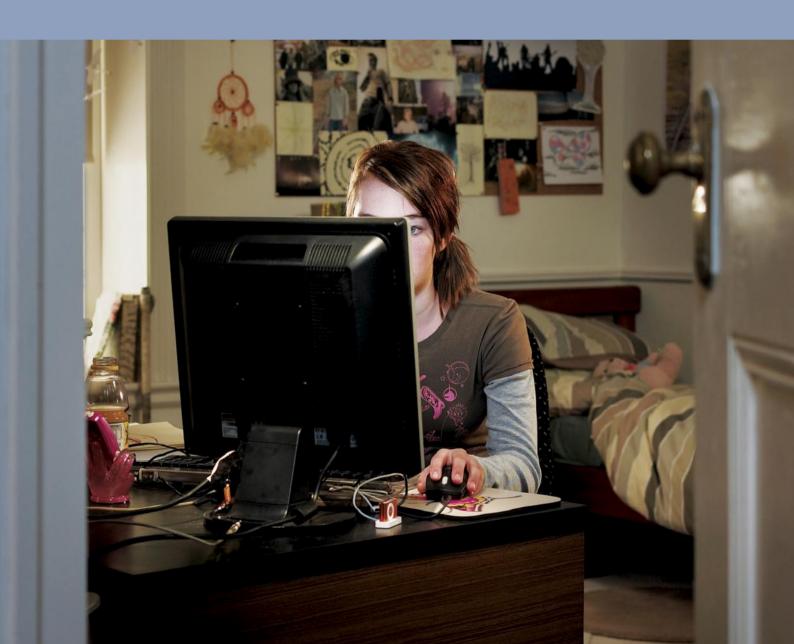


# NetAlert Protecting Australian Families Online



# Contents

Message from the Prime Minister	2
NetAlert – Protecting Australian Families Online	4
Your family – your choice	5
SEE your way to internet safety	6
How can you help protect your children online?	7
Online grooming  Do you know who your children are meeting online?	8
Online abuse It's easy for personal information to fall into wrong hands	10
Inappropriate material Inappropriate content is never far away online	12
<b>Cyber bullying</b> Young people can be harassed and bullied online	14
Online security	16
Internet content filters	18
Glossary of words and terms	20
Who to contact to keep your family safe online	23

# NetAlert Protecting Australian Families Online

www.australia.gov.au/netalert 1800 880 176

# Message from the Prime Minister

The internet is a window on the world that has transformed the way we communicate. Properly harnessed, it has enormous potential as a tool for education, entertainment, interaction and global engagement.

Just like the real world, though, there is a lot on the World Wide Web that you wouldn't want your children to see or be a part of. Offensive materials are just a few mouse clicks away and not everyone your children meet online can be trusted.



There are some simple steps that can minimise the risk of exposure to inappropriate material and prevent young people from accessing and creating illegal content.

Parents and carers can protect their children by talking to them about what they are doing online and by supervising internet usage. They can educate children about the potential dangers on the internet and equip the family with online protection by installing Internet content filters. It's also important for families to keep their computers secure against harmful emails, viruses and unauthorised access.

There is nothing more important than ensuring our children are safe. That's why the Australian Government has created the \$189-million NetAlert – Protecting Australian Families Online program. This program combines education, parental support and the offer of free internet content filters – all effective tools to help protect children from illegal and offensive material online.

This booklet contains information about the software available and ideas about how to begin a conversation about internet safety with your family. Please read it and hold onto it for further reference and use the resources offered within it.

Importantly, we must recognise that while the free services we are providing, such as customisable filters, a web portal and a contact centre, will be useful tools for families, traditional parenting methods are more important than ever. I encourage parents to discuss online safety with each other and with other carers of their children including teachers, babysitters and grandparents, but most importantly, let's start the conversation with your children.

John Howard

John Haward

# Your family – your choice

# **NetAlert – Protecting Australian Families Online**

The Australian Government has developed the \$189-million *NetAlert – Protecting Australian Families Online* initiative as a multi-faceted response, combining services and education, regulation and policing to ensure that Australian families can get the best from the internet, whilst minimising potential harm.

Tackling the dangerous side of the internet falls into two main categories: the content available online and, most concerning, the potential for online predators to contact unsuspecting children.



Importantly, parents and carers of children should be aware that there is no one single solution for this myriad of potential dangers.

Equally, in the context of legal content, what may be considered appropriate material for some might not be acceptable for others, as values differ from individual to individual.

NetAlert – Protecting Australian Families Online will help you tailor your family's internet experience in a way that is compatible with your needs and values by providing:

- information and advice on internet safety strategies for your family
- free internet content filtering for your home computer
- advice on how to make a complaint about prohibited online content or illegal online activity.

Through *NetAlert – Protecting Australian Families Online* the Australian Government is bringing world-class internet safety information and technology to families and strengthening measures to fight internet-related crimes against children.

However, whilst we have an enviable world reputation in online safety, the pace of social change and developments in technology mean we must continue to be vigilant.

Education about online safety is important for you and your family. You can help to make your children aware of the risks in the online environment and give them the skills and support they need to handle them. But first, you need to learn about the potential dangers for your children online and what tools are available.

So, let's open the discussion.

# NetAlert - Protecting Australian Families Online program elements

#### **National Filter Scheme**

\$84.8 million to provide access to the best available internet filtering technology, free to every Australian family through PC-based or ISP-based filtering and for public libraries

# Law enforcement and prosecution

- \$43.5 million over four years additional funding for the Australian Federal Police (AFP) to combat online child sex exploitation
- \$1.4 million for the Commonwealth Department of Public Prosecutions in year one and \$2.8 million thereafter to deal with increased activity by the AFP's Online Child Sex Exploitation Team (OCSET)
- Australian Government to lead a Consultative Working Group comprising government, education, community and industry representatives to address the use of social networking sites for predatory contact with children

# **Increased regulation**

- Funding to the Australian Communications and Media Authority (ACMA) of more than \$7.1 million to deal with additional investigations into online content, expansion of the ACMA black list and *NetAlert* resourcing
- \$0.5 million for Australia to take a lead in finding new and more effective methods to deal with illegal content hosted overseas

# Program of support, education and awareness

- More than \$9.2 million for *NetAlert* to provide internet safety advice, a dedicated family support help line and a website
- More than \$22 million over three years to raise public awareness of issues, educate parents and carers and create partnerships with law enforcement agencies, schools and community groups
- \$11.7 million over four years to treble the *NetAlert* ACMA School Outreach Program

# SEE your way to internet safety

Follow these three steps for internet safety:

**S**upervise, **E**ducate and **E**quip (SEE) your family to stay safe online.

# Supervise your children

Supervise your children on the internet and set and stick to rules about appropriate use.

Together with your children, set house rules about what they are allowed to use the internet for, how they interact with people online and what information they are allowed to give out. You can formalise these in an internet safety contract which both you and your children sign. Regularly discuss and review the rules to make sure your children are able to access what they need or want in a safe manner.

Build good habits about internet usage from an early age. Place household computers in family areas so that children get used to using the internet openly.

# **E**ducate yourself and your family

Educate yourself and your family about potential dangers online and teach them the skills they need to handle such dangers. Children and young people need to be encouraged to think carefully and critically about everything they encounter online, so that they make the right choices about online behaviour.

# **Equip your family**

Equip your family with online protection to help you manage your family's online experience. Keep your computer secure.

For practical internet safety advice or to download a free internet content filter go to www.australia.gov.au/netalert or ring 1800 880 176.



# Protecting children online



# How can you help protect your children online?

### Children aged under 8

- Check out good sites for younger children you should be responsible for selecting the sites that children in this age group can visit and you can bookmark these sites to encourage children to visit them
- Very close supervision is strongly recommended
- Consider using 'safe zone' websites which are designed specifically for children, 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



# Children aged 8-12

- Be actively involved in your child's internet use
- Emphasise safe online behaviour and discuss why it is necessary
- Investigate chat rooms or online clubs your child wants to join to make sure they are legitimate
- Consider using filters to block access to instant messaging (IM) and newsgroups
- Discuss use of good cyber manners (netiquette), just as you do for the real world
- Place the computer in a public area of the home to supervise children's use
- Use family-friendly search engines designed for children



# Children aged 13-17

- 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 younger teens in particular should be reminded about the need to protect private information, including anything that might provide clues to their identity
- Ensure that teens understand that posting to newsgroups makes their email address public

# Online grooming

# Do you know who your children are meeting online?

Rebecca, a young girl, met a sex offender using an online chat program.

The man posed as a teenage boy and communicated with her over several months, leaving money and gifts for her to find in a local bus shelter.

When they finally met, Rebecca realised she had been lied to and told her parents, who reported the matter to the police.\*

The most serious risk for children while they are online is coming into contact with sexual predators. You can take action to reduce the risk of your children meeting someone like this.

- Talk to your children about 'stranger danger' online. Most children know not to respond to a stranger who approaches them on the street. Unfortunately, it's easy for young people to feel that they know someone well in a very short time online
- Explain to young people that they must never agree to meet anyone they've met online in person without your permission
- Contact the police if you think a young person may have come into contact with a predator online

In a recent study, 40 per cent of children who chat online said they had been contacted by someone they didn't know<sup>†</sup>

#### What is a chat room?

A chat room is a place on the internet where people with similar interests can meet and communicate by typing messages into their computer. Messages typed in by a user appear instantly to everybody who is in that chat room.

Chat rooms are very popular with both young people and adults. Most people in chat rooms are there for genuine reasons. However, chat rooms are essentially anonymous and it is not always possible to know if someone really is who they say they are.



# What is instant messaging (IM)?

An instant messaging program sends messages and/or files from one computer to another. They are a form of 'instant email' that indicates when friends or family are online, and allows you to send them short messages, similar to sending an SMS text message on a mobile phone.

Many children use these programs to chat to their friends after school or on weekends.

Instant messaging programs are usually a one-to-one communication, although some programs allow many people to chat to each other at the same time, much like in a chat room.

#### What is social networking?

Social networking websites are like online diaries. They encourage people to create profiles of themselves, communicate with others and form online networks of friends. Profiles may contain personal information such as photos and descriptive comments about the member.

They also make it easy for children to make new friends and communicate with existing ones from the comfort of their own computer.

#### **Supervise Educate** Set up an internet safety If your child is Helpful filter functions: plan for effective use of uncomfortable with Block chat or the internet and chat something happening on peer-to-peer messaging rooms at home the internet, teach them Block internet to say no and encourage Ensure your children applications such as them to speak up only share their real VOIP (Voice Over identity with known Learn the terms your Internet Protocol), and trusted people children are using, so chat rooms, games, you can talk to them Many schools require newsgroups etc. in the language they their students to sign Allows different settings understand an Acceptable Usage for different users Policy before they can Experience first-hand Easy updating of profiles use the internet what chat rooms are and Block access at how they work predetermined times or after a nominated period of time Provide detailed reporting of other online activity by different users

# Online abuse



Personal information in the wrong hands can lead to online abuse

Sarah met a man in an online chat room and gave him her email address. He started sending her abusive messages and explicit photographs of himself.

He was also able to discover her mobile phone number and her netball team's playing schedule from other pieces of information Sarah had placed online.

Sarah had to change her email address and phone number and her family reported the harassment to police.\*

Once your child posts their address, phone number or photograph online, it's very difficult to control who sees that personal information. There are a range of popular and increasingly sophisticated search engines that can search the internet for references to your child's involvement in clubs and sports in both the real and online worlds.

Here are some steps you can take to ensure your child's details don't end up in the wrong hands.

- Encourage your children to use anonymous online names that don't reveal their age, gender or location
- Talk to your children about the information they make available online
- Young people who place private photographs or diaries on personal sites should be encouraged to restrict access, so that only users on an approved 'friends' list can see them
- Children should be cautious about who they invite to join their 'friends' list
- Be careful with webcams.
   If you have a webcam at home, don't advertise it and only use the webcam with real friends and family



# In a recent study, 39 per cent of children said they had put a photo of themselves online.<sup>†</sup>

Supervise	Educate	Equip
Reinforce safety messages and cyber rules	Remind children about the need to protect private information, including anything that might provide clues to their identity	Helpful filter functions:  Block sending of personal information

# Inappropriate material

# Inappropriate content is never far away online

An eight-year old boy came across offensive images when he innocently conducted an internet search for films about boys.

Devastated and afraid he would get into trouble, he initially refused to explain why he was upset when his mother discovered him in tears at bedtime.

His parents contacted NetAlert for advice on how to block sites with inappropriate content.\*

Whether intentionally or accidentally, disturbing images of extreme violence and pornography are never far away online. Also, some radical groups use the internet to promote extreme opinions and young people might not question the truth of what they read online. Offensive material can also be swapped using

peer-to-peer file sharing software and internet chat programs.

There are steps you can take to help protect your family from distressing content:

- Teach children not to open emails or files from unknown sources – spam emails can contain links to explicit material and some viruses and spyware can change your internet settings to direct you to inappropriate sites
- Encourage young people especially young children to come to you if they encounter something disturbing or traumatic online
- Download a free internet content filter to help block, monitor and screen inappropriate websites on your home computer

Remember that an increasing number of mobile phones also provide access to the internet. Unfortunately, internet content filter technology for mobile phones is still developing.

New safeguards to protect consumers from inappropriate or harmful material on convergent devices, such as mobile phones and services available through subscription internet portals, are expected to come into effect over the next few months.

Who to contact: If you come across a website you think might be breaking the law, contact the Australian Communications and Media Authority (ACMA). Contact details are at the back of this booklet.



# Supervise

- Check out good sites for younger children and set up a white list that limits access to only those websites
- Alternatively, bookmark these sites and encourage your children to visit them

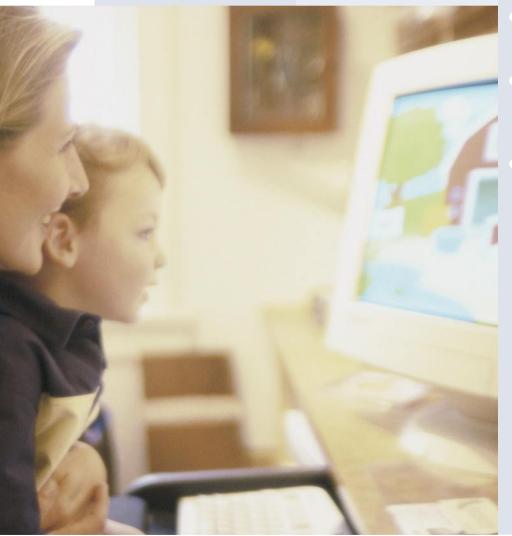
#### Educate

- If your child sees something online that makes them feel uncomfortable, encourage them to speak up
- Talk to your children about their expected behaviour when they roam the internet

#### Equip

### Helpful filter functions:

- Block website content according to a range of categories
- Set access to only specific sites – sometimes referred to as a white list
- Allow different settings for different users
- Set up different profiles for each child who uses the computer
- Block access at predetermined times or after a nominated period of time
- Provide detailed reporting of internet usage and other online activity by different users



# Cyber bullying

# Young people can be harassed and bullied online

When Lauren had a falling out with her friend Susan, Susan used Lauren's private instant messenger account to send nasty messages to her classmates at school.

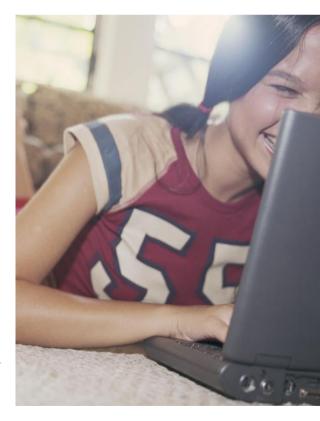
Suddenly, Lauren's friends were ignoring her, and vicious rumours about Lauren began to circulate through SMS, online notice boards and web pages.

Working with her school, Lauren's family were able to put a stop to the bullying, but the damage had been done and Lauren lost a lot of friends.\*

Online or cyber bullying is carried out through an internet service such as email, a chat room, discussion group, social networking site or instant messaging. It can also include bullying through mobile phone technologies such as SMS. This is a serious problem, but parents can help to stop this kind of harassment.

In a recent study, 1 in 5 children aged 13–17 said they had seen or heard people bullying or abusing other people online.<sup>†</sup>

- Talk to your children about how they behave online
- Hurtful comments and nasty rumours spread through text message or chat programs are just as damaging as those made in real life
- Tell your children not to reply to bullying messages
- Change their contact details and get a new user name for the internet, a new email account and a new mobile phone number which they only give out to their closest friends
- Remind your children to keep their user name and passwords secret so they do not fall into the hands of someone who could misuse them
- Keep a record of any worrying emails or online messages (including time and date) to help you (or the police) find out who is sending the messages
- Check the Terms of Use policies on websites in many cases, reporting bullying or threatening behaviour can result in a perpetrator's account being deleted



If messages are threatening or serious get in touch with the police. You should also contact your phone or internet service provider and report what is happening as they can help block messages or calls from certain senders.



#### Supervise

- Stay in touch with what your children are doing online by discussing internet issues and sharing internet experiences
- Watch out for any behaviour changes, especially related to online activity

#### **Educate**

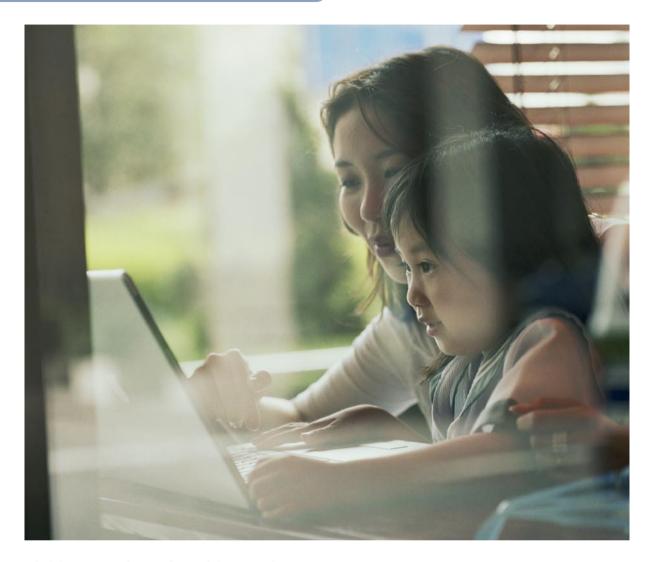
- If your child is being bullied, encourage them to let someone know
- Reinforce safety messages and cyber rules
- Know who to contact if your child is being cyber-bullied and what the procedure is for removing distressing information from the internet

#### Equip

#### Helpful filter functions:

- Block chat or peer-to-peer messaging
- Block internet applications such as VOIP, chat rooms, games, newsgroups etc.
- Provide detailed reporting of other online activity by different users

# Online security



Children are also vulnerable to online scams

When Matthew downloaded free software from the internet, he didn't realise he had also downloaded a piece of spyware.

The spyware program collected information from his computer and sent it on to someone who accessed Matthew's email and internet banking without his knowledge.\*

Like adults, young people can be tricked into responding to online scams, opening files that infect computers with viruses or passing on confidential information to untrustworthy sites.

- Talk to your children about the dangers of downloading material from dubious sources
- Use internet security software to block unwanted junk emails, known as spam, and downloads containing scams and viruses

### **Securing your computer**

It's not just parents and carers with children who need to worry about online safety. Keeping your computer secure is an important issue for everyone.

If you don't protect your computer properly, you are putting yourself and possibly your family and friends at risk.

Take some time to protect your computer from harmful emails and viruses and from unauthorised people getting access to your internet connection and your information by following these steps:

- Set and protect passwords for your computer and online transactions
- Use and update anti-virus software
- Use and update anti-spyware software
- Consider installing and using a firewall
- Learn about the safety settings for your internet browser and set them so they provide you with protection online
- Learn about managing and blocking unwanted emails (spam)
- Turn off your internet connection when you are not using it

There are more smart practices you can follow to make banking, buying and selling things on the internet as safe as possible.

Who to contact: You can find out more about the risks for children in the online environment at www.australia.gov.au/netalert or by calling 1800 880 176.

For more information on how to secure your computer or safe transacting online visit www.staysmartonline.gov.au

Supervise	Educate	Equip
Keep your children informed about new security risks and scams	Children need to be educated about identity theft just as they do about any other internet safety issues	Helpful filter functions:  Block sending of personal information

# Internet content filters

An internet content filter is a piece of software that helps you manage access to online content on your home computer. Installing an internet content filter reduces the risk of your family coming into contact with something upsetting or dangerous online but – like a seat belt in a car – it does not offer total protection.

Internet content filters offer a range of different functions to help block, screen or monitor unwanted material. Unfortunately, there is no single action or internet content filter that does everything and it's not possible to have two or more internet content filters installed on your computer at the same time. At present, internet content filter technology is still being developed for use with mobile phones.

Remember that a single filter may not offer you all you need and you cannot use more than one filter at a time. It's important to choose the one most relevant to your family's needs. More detailed internet safety strategies and a filter comparison table are available at *www australia.gov.au/netalert*, or by ringing 1800 880 176, to help you make the best choice for your family.



### **Blocking**

Some internet content filters use a variety of techniques to detect unwelcome content including 'black' or 'exclusion' lists to block access to content. These black or exclusion lists contain websites or website pages that have been deemed to carry inappropriate content such as pornographic or violent images. If the user types in an internet address or clicks on a link to content which is on a black list, they will be blocked from viewing that content. Many filters allow the user to set different categories of blocking for different

ages and family values.

The Australian Communications and Media Authority (ACMA) regularly updates a list of prohibited content that will be blocked completely by the free internet content filters being provided by the Australian Government's NetAlert – Protecting Australian Families Online initiative. Also, most internet content filter providers maintain their own list of unwelcome material.

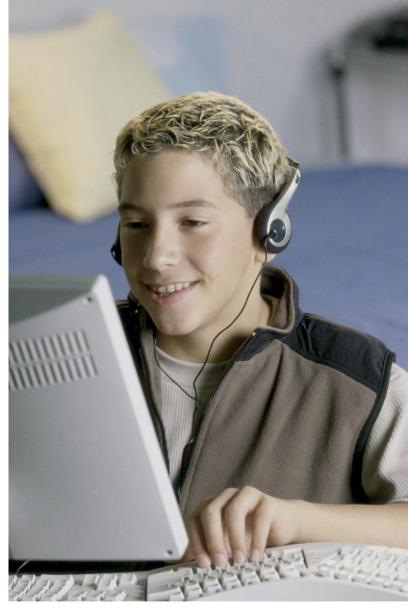
Some internet content filters are also able to block chat, instant messaging and email communications.

# **Screening**

Some internet content filters also use more advanced techniques including key word and phrase searches to help screen out offensive content that has not been included on a black or exclusion list. You can set filters to help screen other content based on your family's values and concerns.

# Monitoring

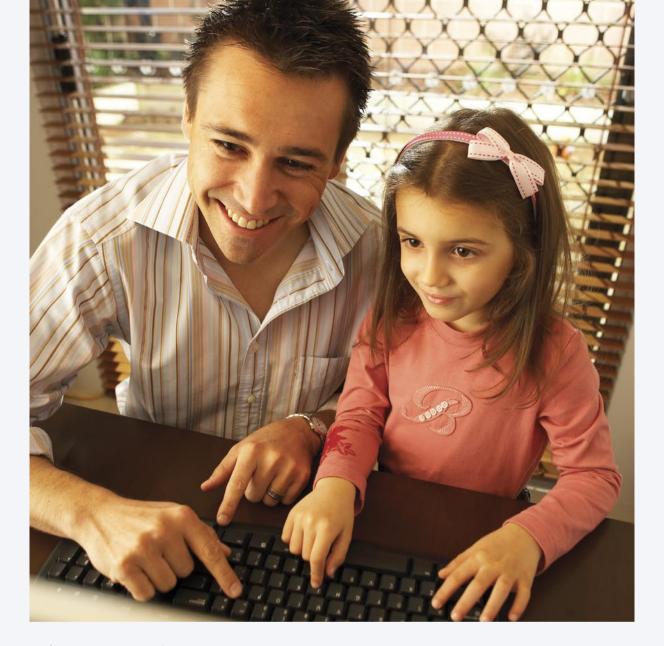
Some internet content filters allow monitoring of user activities such as programs used, websites visited, chat room activity and social network sites accessed.



Who to contact: For more information on internet safety plus free filters go to www.australia.gov.au/netalert or phone or call 1800 880 176.

# Glossary of words and terms

- **Anti-virus software** A program that searches computer memory, hard drives and floppy disks for any known or potential viruses and removes or disables the viruses.
- **Black list/exclusion list** A list of website addresses or domain names which will be blocked by a filter.
- **Browser** A program that allows a user to find, view, hear and interact with material on the internet.
- **Chat** Live communication over the internet. As one person enters text it appears on the other person's screen in real time, or almost instantly.
- **Chat room** A place on the internet where people with similar interests can communicate in real time by typing messages on their computers, sometimes requiring special chat software. Anyone can join open chat rooms without any robust verification of identity or age.
- **Cyber bullying** Bullying which is carried out through an internet service such as email, chat room, discussion group, instant messaging or a mobile phone.
- **Cyber stalking** Stalking or harassment by one person to another person using a service of the internet such as email, instant messaging or through a posting in a discussion group.
- **Firewall** Software or hardware that limits certain kinds of access to a computer from a network or other outside source.
- **Identity theft** A crime in which an impostor obtains key pieces of personal information, such as credit card or driver's licence numbers to impersonate someone else.
- Instant messaging (IM) An instant messaging program can instantly send messages and/or files (such as photos) from one computer to another. Examples of IM services are, Yahoo Instant Messenger, AOL Instant Messenger, ICQ, MSN Messenger and internet relay chat.
- Internet content Internet content may consist of text, still pictures, moving pictures or computer games. Internet content does not generally include ordinary email or information that is accessed in real time without being previously stored, such as chat services and VOIP.
- **Key words** Words that are used by an internet content filter to determine if a page can be displayed. If a word is on a black list, and is contained on a webpage, the user may be denied access to that webpage. See also 'black list' for more information.
- **NetAlert ACMA Schools Outreach Program** *NetAlert* trainers will visit schools and community groups in every state and territory throughout Australia. The program will provide parents and teachers with hands-on support and practical internet safety assistance, to help them ensure their children's or students' internet experience is a safe one.
- **Newsgroups, discussion group etc.** A site on the internet where people can contribute to discussions on subjects of shared interest. Unlike chat rooms or instant messaging, these internet forums and discussion groups do not operate in real time.



**Online grooming** – Conduct which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes. The online groomer is a person who uses the internet to contact a child with the intention of establishing a sexual relationship involving cyber sex or physical sex.

**Operating system** – A computer program that manages all the other programs that are installed on the machine. Operating systems perform basic tasks such as recognising keyboard strokes, displaying information on a screen, storing files and directories of files and controlling other hardware such as printers, scanners or disk drives. Different types and versions of operating systems are available, such as Windows or Mac OS.

**Peer-to-peer (P2P) –** Peer-to-peer networks are online communities where members share, search and download files which are located on their computers.

**Personal information** – Internet content filters can prevent the sending of certain types of personal information. The user can configure which information is not to be transmitted, such as specific names, addresses, phone numbers and credit card numbers. If this information is typed into the computer such as in an online form, email, or chat conversation, the program will block the information from being sent over the internet.

- **Prohibited content** Prohibited internet content falls within the classifications RC (refused classification) or X 18+. The Australian Government's online content regulatory scheme allows the Australian Communications and Media Authority (ACMA) to require websites hosted in Australia to take down prohibited material. A third category of strong content, classified as R18+, is also regulated. Recently, new legislation has also been developed that will extend the current protections so that MA15+ material, if made available for a fee, must be provided with age restrictions designed to limit children's exposure to such material.
- **Social networking** A term given to a range of new generation internet services and applications. Websites are created that enable users to register and provide details about themselves with diaries/journals, images, text, video and audio. These sites can be restricted to 'invitation only' friends lists or can be open for browsing by anyone on the internet. Some social networking applications are also programs that require installation on the computer which allow the user to enter virtual environments and interact with other users.
- **Spam** Spam is the common term for electronic 'junk mail' unsolicited commercial electronic messages. *The Spam Act 2003* prohibits the sending of spam (identified as a commercial electronic message sent without the consent of the addressee through email, SMS, multimedia message service or instant messaging. Individuals or businesses can report spam to the Australian Communications and Media Authority (ACMA) at <a href="https://www.acma.gov.au/spam">www.acma.gov.au/spam</a>. SpamMATTERS is software that users can install to submit spam directly to ACMA's complaints database.
- **Spyware** Software that is installed on a computer and takes information from it without the consent or knowledge of the user. It is used to literally spy on people and collect information about them. People who install spyware may target information such as banking and credit card details or other sensitive, commercial or private information. They may take this information for their own use or give it to another person. Anti-spyware software is available.
- **URL** A universal resource locator is a computer address that identifies the location and type of resource on the internet. A URL generally starts with 'http'.
- **VOIP** Voice Over Internet Protocol enables internet users to place voice calls to each other, similar to a normal telephone services, through the computer. VOIP programs can incorporate instant messaging functions. They can indicate when friends or family are online and enable video calls.
- White list/inclusion list Lists of approved sites that can be accessed from the computer. You choose the site on the approved list and all other sites are blocked.



# Who to contact to keep your family safe online

# For internet safety advice

The *NetAlert* program was established by the Australian Government in late 1999 to provide independent advice and education on internet safety and managing access to online content. It provides young people and parents with information and advice about the issues, risks and dangers associated with using the internet.

Who to contact: For practical safety advice or to download a free filter go to www australia gov au/netalert or call 1800 880 176

# To report prohibited internet content

You can report online material you think should be prohibited to the Australian Communications and Media Authority (ACMA). All valid complaints will be investigated and ACMA may place offending sites on a black list.

Who to contact: For more information, or to make a complaint, visit www.acma.gov.au/hotline

# To report illegal activities

The Australian Federal Police (AFP) Online Child Sex Exploitation Team is responsible for the investigation of Australian websites that exploit children, including child pornography, abuse and grooming. The AFP will refer any sites not within Australia to overseas law enforcement agencies. The AFP is a member of the Virtual Global Taskforce which is made up of police forces from around the world working together to fight online child abuse. Who to contact: If you know of a child who is in immediate danger or risk, call 000 or your local police. You can report any concerns about suspicious or inappropriate behaviour online to the AFP at www.afp.gov.au/online\_forms/ocset\_form To report any information to police call Crime Stoppers 1800 333 000.



# www.australia.gov.au/netalert 1800 880 176

Interpreters and TTY facilities available

