

# A Parent's Guide to Internet Safety

Produced by NetAlert  
[www.netalert.net.au](http://www.netalert.net.au)

## Introduction to Internet safety

The Internet offers an enormous range of opportunities for today's children. Instant communication, information discovery and online publishing, open up a world of excitement and happiness for children of all ages. Ease of access, affordability and mobility makes the Internet an everyday part of their lives.

Parents recognise the **benefits** but are also concerned about the **potential dangers** in the online world.

News spreads quickly through the media when a serious incident happens to a child on the Internet and parents concerns are justifiably heightened. Never the less, parents should keep this in perspective and remember with a sound grounding in Internet safety, children will develop techniques that will protect them from many online hazards.

The **challenge for parents** is to be aware of potential dangers and to be **equipped with solutions** to help their children enjoy the Internet. Developing an Internet safety management plan to help control access to the Internet is essential for parents who want their children to remain safe online.

NetAlert has prepared this parents online safety guide as a resource to help you create your own Internet safety strategy for your family. Whether you are simply investigating the issues or need some practical advice on how you can help your children, this guide is for you!

## Contents

1. What is the Internet?	pg.1
2. What services are on the Internet?	pg.2
3. Children and the Internet.	pg.2
4. What are children aged 2-7 doing online?	pg.3
5. What are children aged 8-11 doing online?	pg.4
6. What are children aged 12-18 doing online?	pg.4
7. What are the risks my children face online?	pg.5
8. Online paedophiles.	pg.6
9. What are the danger signs with my children?	pg.6
10. The different approaches to Internet safety.	pg.7
11. Strategies to help protect your children online.	pg.8
12. Who is NetAlert?	pg.9
13. What NetAlert can do to help.	pg.10

## 1. What is the Internet?

The Internet is a global network of computers linked together which are able to communicate through telephone lines, cables and satellites.

Information in the form of text, pictures, movies and voice are transmitted and shared between people who are connected to the Internet.

There is no central 'home' for the Internet as it has been designed to operate from many geographically different locations. Anybody can connect to the Internet if they have an Internet ready computer and an account with an 'Internet Service Provider'.

No organisation or individual owns the Internet but countries can legislate regarding usage or the content.

## 2. What services are on the Internet?

There are a number of activities people can do when they are connected to the Internet. These activities are called 'Internet Services'. Innovative Internet services develop as technology advances and 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 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). People using email require an email address, which identifies them as a unique person online. 'Internet Service Provider's' supply email addresses to people when they open an Internet account;
- **Chat** – used to send instant messages to other people on the Internet. Messages can be sent to friends or strangers. 'Chat rooms' are places on the Internet where people congregate together online and send messages back and forth to each other; and
- **Newsgroups** - places on the Internet where people can post messages about a topic. People with a similar interest 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).

## 3. Children and the Internet

Children today are exposed to the Internet at an early age and from a variety of places, which can include:

- **School** - computers can be found in all levels of the education system;
- **Home** - many homes now have personal computers and Internet access;
- **Friends** - if your child does not have access to the Internet at home, there is a high chance that one of their friends will have an Internet connection;
- **Libraries** - libraries have Internet terminals for use by patrons;
- **Public Access Centres** - public places where members of a community can gain access to the Internet; and
- **Mobile Internet enabled devices** - mobile devices such as phones are now able to access the Internet.

With so many places available for children to connect to the Internet, it is virtually impossible to deny them access. As a result, parents need to prepare children for Internet safety, just as they do other forms of child safety such as crossing the road or how to act in an emergency.

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

#### **4. What are children aged 2-7 doing online?**

Preschoolers can begin to explore the Internet and to learn about the computer. Sit with them and teach them Internet navigation and computer skills via educational games on appropriate web sites.

Children from about 5 years may start to visit children's web sites with you and to enjoy email correspondence with family and friends (a great way to start learning keyboard skills).

##### **What parents can do:**

- Check out good sites for young ones - 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 you have approved; and
- Use filters to limit accidental access to unsuitable material.

## **5. What are children aged 8-11 doing online?**

From around 8 years old children can 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 how to deal with it. Whilst their skills and independence are increasing, making Internet exploration a family activity allows you to maintain close supervision.

### **What parents can do:**

- Be actively involved in your child's Internet use;
- Emphasise the 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) just as you do for the real world;
- Place the computer in a public area of the home to help keep an eye on what's going on; and
- Use search engines designed for children.

## **6. 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 or blocking software and attempt to access 'forbidden' material.

Many are 'Net savvy'. They know about hacking into systems and understand basic computer programming. 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 in the home. It helps to be able to keep an eye on what is going on;
- Reinforce safety messages and cyber rules. Younger teenagers in particular should be reminded of the need to protect their privacy;
- Ensure teens understand that posting to newsgroups makes their email address public. Have them change their email address if they suspect they are being tracked; and
- Ensure both you and your teenagers understand laws relating to copyright, privacy, software piracy, hacking and obscenity.

## **7. What are the risks that my children face online?**

There is a number of risks children face when online, which are common in many Internet services such as chat rooms, email and web browsing.

The risks can include:

- **Privacy** - children can be very trusting on the Internet and distribute their personal information without concerns;
- **Security** - when online, children can be exposed to viruses (computer programs that cause havoc to computer system) and hackers (people that try to break into computers);
- **Cyber bullying** - many of the traditional bullying behaviours are now being used online and children are vulnerable to online pressures applied, usually by their peers;
- **Online grooming** - individuals (usually adults) who will try to make online contact with children, for the purpose of their own sexual exploitation;
- **Inappropriate content** - children can be exposed to material that is inappropriate including pornography, advertising material, violence, hatred and extremist groups;

- **Online scams** - scams are conducted online as they are in the real world, except the scammers usually do not care about the age of the person they are scamming – they are simply interested in what they can get out of somebody;
- **Psychological problems** - children can become addicted to the Internet and have trouble socialising with others either at home or in school;
- **Electronic crime** - children can become involved in illegal online activity. Often they are unaware what the legal, moral and ethical issues are; and
- **Identity theft** – another person can steal a child's identity and perform illegal activity online.

## 8. Online paedophiles

Along with risks such as viewing inappropriate content or being bullied online, parents are concerned about their children being contacted by a paedophile online. Paedophiles find the Internet attractive because they can remain virtually anonymous whilst participating in a range of paedophilic activity, such as making contact with children.

Paedophiles pretend to be people other than themselves and find a sense of security by operating from the confines of their own homes. They often set up bogus 'email accounts' and 'chat handles' which protect their identity online. Paedophiles can also erase the history of what they have done online from their personal computers, making it a lengthy task for authorities to charge them with an offence.

Parents need to be aware of 'online grooming' and know that paedophiles use the Internet as a way to make contact with children.

## 9. What are the danger signs with my children?

Children's behaviour in the real world can change if they are at risk online. Children often transmit danger signs and if parents are aware of these, serious problems can be avoided.

Look out for the following if you think your child is at risk online:

- Spending **large amounts of time** on the computer - an indication that children might have discovered an area of the Internet that involves excitement or risk;
- **Minimising the screen** when you walk past - this type of behaviour may indicate that inappropriate content such as pornography or violence could be being viewed;
- Your child is **angry or depressed after being online** - a cyber bullying incident might have occurred online that has upset your child;

- **Staying up late at night** - children will often wait until parents are out of sight before experimenting with risky behaviour;
- Spending a lot of **time alone online** - children can form online relationships or be 'groomed online' by adults. Children like to be alone when forming serious relationships;
- Excessive use of **chat rooms** and **instant messaging** - using the computer for communication is similar to using the phone. Be alert that your child may be talking to strangers who could be adults with hidden motives;
- **Unusual mail** is delivered - parcels or letters from strangers appear in the mail. Your child could have met somebody online and now the person is making real life contact;
- Your child is sending **excessive amounts of SMS messages**, or their mobile phones are constantly ringing - this behaviour could indicate a relationship has formed in the real world; and
- **Excessive use of other technology** - children can all of a sudden start scanning in pictures, copying disks, burning CD's and DVD's. Something must be happening - investigate to see if it is just harmless fun or something more serious.

There are other behaviours that can change depending on each individual child's situation. Talk to other parents and see if there are any give away signs that they have noticed with their children when they suspected trouble online.

## 10. The different approaches to Internet safety

There are a number of different approaches, which can be used to develop an Internet safety plan for your family. A mixture of these will give the best overall result and protection.

The approaches can include:

### Technological approach:

- **Filters** - software that helps manage online access and block inappropriate content;
- **Labelling** - setting up your Internet browser so that sites that labelled inappropriate can not be viewed;
- **Monitoring software** - software that keeps track of online activities; and
- **Telecommunications** - ways in which your Internet Service Provider or telecommunications carrier can help;

### **Educational approach:**

- **Instructional materials** - teaching resources such as books and video's;
- **Fun activities** - activities that help children learn about Internet safety through engaging their interests; and
- **Peer groups** - children learning appropriate online behaviour from their peers.

### **Family approach:**

- **Discussions** - talking to children about the benefits and potential dangers of being online;
- **Online contracts** - creating family contracts that can limit the amount of time spent online and outline expected levels of behaviour; and
- **Supervision** - techniques to supervise children's access to the Internet.

### **Legal approach:**

- **Being proactive** - knowing the legalities for appropriate online behaviour; and
- **Reporting trouble** - knowing who and what to report if trouble is encountered online. A strategy could involve contacting family and friends, law enforcement agencies and government.

Using a range of Internet safety approaches will provide the best overall protection for your children online. Select the approaches which are appropriate to your family situation, as every parent will have different requirements.

## **11. Strategies to help protect your children online**

Children need parents and carers to help teach them how to stay safe online.

Here are some general tips for parents to use:

- Spend time online with your children. Check out good sites together. The Internet can be a fun family activity;
- Help your children use the Internet as an effective research tool - learn about handy homework tips for children and also good searching ideas;
- Be aware of online stranger danger, particularly in chat rooms. Set house rules about what information your children can give out and where they can go online;

- Put the Internet computer in a public area of the home, such as the living room, rather than a child's bedroom;
- Talk to your children about their Internet experiences, the good and the bad. Let them know it is OK to tell you if they come across something that worries them. (It does not necessarily mean that they are going to get into trouble.);
- Teach your children that there are ways they can deal with disturbing material - they should not respond if someone says something inappropriate and they should immediately exit any site if they feel uncomfortable or worried by it;
- Teach children that information on the Internet is not always reliable;
- Encourage children to treat others in the same way that they would in real life by giving them an understanding of netiquette;
- Know the best ways of avoiding spam;
- Consider using filters, labels and safe zones; and
- Set some appropriate guidelines for Internet use and discuss them with children you care for.

Children need parents and carers to teach them how to make smart choices about who and what they find online, how to deal with commercial material, how to safeguard their privacy, how to have a positive experience when meeting people online, and how to use their time on the Internet effectively.

The types of rules you may have made about dealing with strangers and what children can watch on television or video are also relevant to the Internet.

## 12. Who is NetAlert?

NetAlert Limited (NetAlert) is the Australian Internet Safety Advisory Body. NetAlert is a not-for-profit community organisation. NetAlert was established in late 1999 by the Australian government to provide independent advice and education on managing access to online content.

NetAlert's vision is a safer Internet experience, particularly for young people and their families.

Contact NetAlert:

Mailing Address  
NetAlert Limited  
GPO Box 1774  
Hobart Tasmania Australia 7001

Street Address  
NetAlert Limited  
Level 9  
27 Elizabeth Street  
Hobart Tasmania Australia 7000

General enquiries: [enquiries@netalert.net.au](mailto:enquiries@netalert.net.au)  
Website: [www.netalert.net.au](http://www.netalert.net.au)  
Help line In Australia: (toll free) 1800 880 176  
Telephone: +61 3 6234 3312 between 9am and 5pm Monday to Friday EST  
Facsimile: +61 3 6234 1430

### 13. What NetAlert can do to help

NetAlert can help you and your children with Internet safety. The range of services include:

- **Internet safety help line:** A national help line, which advises the community on Internet safety, related issues.

Help line details are:

- Free call: 1800 880 176
- Email: [enquiries@netalert.net.au](mailto:enquiries@netalert.net.au)

If you don't know where to start with Internet safety - or you have a problem and don't know whom to call, ring NetAlert and we can offer advice.

- **Website** - filled with advice on resources on Internet safety. Read advice online or download information sheets or reports on Internet safety. The website also contains an Internet safety directory, cataloging many Internet safety pages from the Internet;

- Web Address: <http://www.netalert.net.au/>
- Internet safety directory: <http://www.netalert.net.au/internet-safety-directory.asp>
- Email: [enquiries@netalert.net.au](mailto:enquiries@netalert.net.au)

- **Internet safety e-newsletter** – a free monthly newsletter that is distributed to parents and families. Deals with a broad range of Internet safety issues;

- Web Address: <http://www.netalert.net.au/00380-Newsletter.asp>

- **Educational materials** - educational materials are available on request. These include posters, information sheets and brochures on Internet safety.

- Free call: 1800 880 176
- Email: [enquiries@netalert.net.au](mailto:enquiries@netalert.net.au)