Australian Government

NetAlert Limited

NetAlert
CyberSafe Schools

A Teacher's Guide to Internet Safety

Foreword

A Teacher's Guide to Internet Safety provides information about teaching safe and responsible use of the Internet in Australian schools. It has been prepared by NetAlert Limited (NetAlert), Australia's Internet safety advisory body.

The teacher's guide considers the dangers associated with using the Internet and the strategies teachers can use to minimise risks. It provides practical information about how educators can teach students safe and responsible use of the Internet. Accompanying the teacher's guide is the CyberSafe Schools Wall Chart for primary and secondary schools. The Wall Chart has been summarised in the CyberSafe Schools Quick Reference Guide which has been formatted to allow teachers to photocopy it for easy reference. The resources should be used in conjunction with each other.
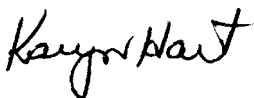
As a Principal of a large secondary school, I understand the demands placed upon teachers in classes to deliver everything on demand, so we have been cognisant of time and availability when developing these resources.

NetAlert 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 is a not-for-profit advisory body. NetAlert is funded by the Australian Government to provide people – particularly young people and parents – with information about the issues, risks and dangers associated with using the Internet. It offers advice about how to minimise risks, avoid problems and use the Internet safely and responsibly.

NetAlert develops and promotes information about technological approaches to managing Internet content for users and the Internet industry. It works closely with Australian Government and State agencies (particularly the Australian Broadcasting Authority), the Internet industry and community organisations in order to promote Internet safety.

The teacher's guide is based on the view that students need to be educated about safe and responsible use of the Internet given the now widespread use of the Internet and Internet-enabled devices by students in schools and at home. It builds on work in the area of Internet safety undertaken by NetAlert, including the development of advice and information websites for parents, children and the Internet industry. The CyberSafe Schools website at http://www.netalert.net.au/schools has been specifically developed for schools. The NetAlert website at http://www.netalert.net.au provides further information about NetAlert's services. It includes a toll free help line on 1800 880 176.

Planning for the development of additional materials to support the current package is under way.

Karyn Hart
Chair

Contents

How to use this guide

A Teacher's Guide to Internet Safety is one of three resources developed by NetAlert to introduce current and trainee teachers to Internet safety issues. The resources provide advice and strategies that will result in sound and safe approaches to teaching and learning while using the Internet.

The teacher's guide has been developed specifically for classroom teachers, school librarians, and school leaders in primary and secondary schools. It has been initially distributed to all Australian schools, along with the CyberSafe Schools Wall Chart and the CyberSafe Schools Quick Reference Guide.

The contents

Educational benefits of the Internet

It is important that students are not only provided with negative messages relating to the Internet. This section provides an overview of some of the teaching and learning benefits of accessing the Internet using a computer or another enabled device.

Internet safety – the issues

There are a range of risks that students may face when accessing the Internet using a computer or another enabled device. These risks apply equally to younger children as well as to older adolescents. The degree of risk may range from exposure to pornographic or illegal content to students placing themselves in situations where they may be exploited by adults. This section describes the kinds of risks that young people may experience.

Managing risks associated with particular technologies

It is easy to concentrate on a few technologies where the risks have been highly publicised. In reality, accessing the Internet using a computer or another enabled device is open to misuse and, when used without guidance, can expose students to unwelcome, inappropriate, racist, or sexist content or approaches. This section explores some of the issues relating to particular technologies and highlights through examples of best practice some of the resources available to Australian teachers and students.

Teaching strategies for Internet safety

Safe use of the Internet should not focus only on what happens in schools, where technological solutions may protect students from inappropriate content, but also on what the student may practise outside the school. Internet safety programs should develop transferable skills that can be used in other environments, such as the home. This section of the guide advises about how to:

* establish a whole school approach to Internet safety
* advice about developing links between school and a range of external environments
* information about where Internet safety teaching fits within the curriculum.

Further resources

Further resources are:

* CyberSafe Schools: Quick Reference Guide for primary and secondary teachers
* an Internet safety glossary
* resources developed by NetAlert, other government agencies/departments, and by the private sector, that are useful when teaching about Internet safety.

Using this resource in your school

One print copy of *A Teacher's Guide to Internet Safety* has been provided to every Australian school. This copy should be catalogued in the library and be available to all staff.

While this work is copyright, permission is given to teachers to make copies of the *Teacher's Guide to Internet Safety* for use within their own school. The CyberSafe Schools Quick Reference Guide has been specially formatted to allow teachers to photocopy it.

Digital copies of the guide are available on the NetAlert website. A digital copy could be downloaded and installed on a school network or Intranet for teachers to use. The Internet address (URL) of the CyberSafe Schools website is (http://www.netalert.net.au/schools).

While some of the content of the guide may be applicable to students, it is not intended that this resource be provided to students or parents. Teachers or school leaders may find it useful to take information such as the CyberSafe Schools Quick Reference Guide (see page 16), and adapt some of it for a non-teacher audience.

Professional development

Schools may find it useful to introduce parts of this resource to teachers in a staged way. This guide or its parts might be introduced or discussed at whole staff, faculty or teaching team meetings.

Audiences for the teacher's guide may be trainee teachers who are new to classroom teaching, or experienced teachers who have used the Internet for teaching and wish to know more about teaching approaches that are informed by safe approaches.

A core resource for teachers within this guide is the CyberSafe Schools Quick Reference Guide, written for both primary and secondary teachers. This is arranged around stages of schooling to take account of the different curriculums of the States and Territories. The quick reference guide does not constitute a curriculum or syllabus, however the information included in it is based on the content of State and Territory curriculum frameworks and syllabuses.

A sample professional development approach

1. Identify a 'champion' or a team within the school with an interest or responsibility for presenting *A Teacher's Guide to Internet Safety* to staff.

2. Introduce this resource and the wall chart at a staff meeting. Distribute the CyberSafe Schools Quick Reference Guide to all teachers. Suggest how they may use and store it. Refer teachers to the NetAlert CyberSafe Schools website.

3. Identify year level or faculty groups who can evaluate how best to incorporate the resource into their teaching programs.

4. Encourage teaching teams to begin an Internet safety project in the classroom and report back to staff.

5. Evaluate and publicise the Internet safety policies and technical solutions made within the school.

6. Communicate and use Internet safety resources with students and parents by, for example, adapting the information in the quick reference guide for the school newsletter.

Educational benefits of the Internet

The Internet provides a powerful resource for learning as well as an efficient means of communication. Its use in education can provide a number of specific learning benefits, including the development of:

- independent learning and research skills – for example improved access to subject learning across a wide range of learning areas, as well as in integrated or cross-curricular studies
- communication and collaboration – for example the ability to use learning technologies to access resources, create resources and communicate with others.

Access to resources

Learning is dependent on the ability to find relevant and reliable information quickly and easily, and to select, interpret and evaluate that information once it is found. Searching for information on the Internet can help to develop these information skills. Classroom exercises and take-home assessment tasks, where students are required to compare and contrast website content, are ideal for alerting students to the requirements of writing for different audiences, the purpose of particular content, identifying bias and judging accuracy and reliability. Since many sites adopt particular views about issues, the Internet is a wonderful mechanism for developing the skills of distinguishing fact from opinion and exploring subjectivity and objectivity.

The Internet is a huge repository of learning material. As a result, it significantly expands the resources available to students beyond the standard print materials found in school libraries. It gives students access to the latest reports on government and non-government websites, including research results, scientific and artistic resources in museums and art galleries, and a whole range of other organisations with information applicable to student learning. At secondary schooling levels, the Internet can be used for undertaking reasonably sophisticated research projects. The Internet is also a time-efficient tool for teachers that expands the possibilities for curriculum development.

Communication and collaboration

The Internet is a powerful tool for developing students' communication and collaboration skills. Above all, the Internet is an effective means of building language skills. Through email, chat rooms and discussion groups, students learn the basic principles of communication in the written form. This gives teachers the opportunity to incorporate Internet-based activities into mainstream literacy programs and bring diversity to their repertoires of teaching strategies. For example, website publishing can be a powerful means of generating enthusiasm for literacy units since most students are motivated by the prospect of having their work posted on a website for public access.

Collaborative projects can be designed to enhance students' literacy skills, mainly through email messaging with their peers from other schools or even other countries. Collaborative projects are also useful for engaging students and providing meaningful learning experiences. In this way, the Internet becomes an effective means of advancing intercultural understanding. Moderated chat rooms and group projects can also provide students with opportunities for collaborative learning.

Numerous protocols govern use of the Internet. Learning these protocols and how to adhere to them helps students understand the rule-based society in which they live and to treat others with respect and decency. The Internet also contributes to students' broader understanding of ICT (information and communication technologies) and its centrality to the information economy and society.

Internet safety – the issues

Despite the educational and social benefits of information and communication technologies, there are risks associated with their use, particularly for school age students. There have been some highly publicised cases of exploitation resulting from unsafe use of the Internet, however this does not mean that all children will experience such problems.

Many children and adolescents accessing the Internet using a computer or another enabled device will be confronted with material that is disturbing or inappropriate. Although there are a range of 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. To instruct children about how to be 'street-smart' and to use the Internet in a safe and responsibly manner is extremely important.

Some potential dangers for young people

Exposure to inappropriate material

Students face the risk of exposure to material that is pornographic, sexually explicit or offensive, hateful or violent, or that encourages activities that are dangerous or illegal. Such materials can be accessed via the World Wide Web or newsgroups, shared in P2P networks, or sent via email or instant messaging services.

Student access of such material may occur inadvertently through searching for educational content about people, places or issues. Teachers should be aware of safe searching techniques and advise students how to deal with unsolicited inappropriate material.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'inappropriate material'.

Physical danger

A risk associated with the Internet is 'stranger danger' – meeting someone online who may claim to be someone they are not. This may occur as a result of a student providing personal information to someone 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 ('online grooming').

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'cyber stalking'.

Commercialism of the Internet and financial risks

The increase in the commercialism of the Internet can be identified in the World Wide Web, in email, in online marketing, or even in gambling. Teaching students how to navigate safely through these elements is essential at all levels of schooling. Some websites are scam sites – they have been set up to deprive people of money or opportunity. Some websites may be bogus or dummy sites, for example websites supposedly for banks but which have been developed to deceive and coax people into providing credit card details ('phishing'). There is the risk that students may put themselves and/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! It is important to stress this with students.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'online shopping', 'e-crime', 'scams' and 'phishing'.

Harassment and bullying

Cyber bullying can be carried out through an Internet service 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 of rumours online, sending unwanted messages and defamation.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'cyber bullying'.

Privacy

Some websites prompt pupils to complete a form on which they are asked to reveal 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 student being targeted for spam (unsolicited email), advertising materials and/or viruses. Privacy issues are also applicable to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illicit purposes.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'privacy'.

Unreliable information

Information on some websites may misrepresent the truth, be out of date, biased or just incorrect. Information literacy requires students to make judgements about the credibility and quality of material they find, or are sent, while online. Racist websites can claim to tell or represent the truth about complex social, cultural or historical issues in ways that appear logical and plausible. Such websites can actively merchandise or even recruit students. Teachers should be aware of the risks associated with particular classroom topics and teach the required information literacy skills, using examples where appropriate.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'unreliable information'.

Spam

'Spam' is the email equivalent of junk mail or nuisance phone calls. Spam can simply be defined as all unsolicited electronic mail sent out in bulk to individuals or organisations that have not consented to receive it. Spam is becoming increasingly prevalent and is an issue for any student 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. Teachers need to teach students to recognise and delete spam without opening it, as spam can include pornographic content or viruses.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'spam'.

Viruses

While email is a useful way of communicating and sharing information, there are risks associated with its use. These include email from unknown senders that contain virus-infected attachments, or following links in an email to a virus-infected website.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'viruses'.

Managing the risks

Internet safety is an issue for all students of school age when using the Internet. The issues are comparable but different in a primary and secondary schools. Some sections below include an example of a resource designed to provide a solution to a particular issue.

The CyberSafe Schools Quick Reference Guide (page 16) relates the development of student skills and knowledge to Internet safety issues for schools and teachers. Each guide is a progress map where student knowledge and Internet safety skills are scaffolded. This map is necessarily indicative as teachers should be conscious of mixed-ability groupings in any given class. Knowledge and skills that are assumed to be taught at lower levels may need to be reinforced to ensure all students can engage with the Internet safely.

Resources for young children

A number of publicly accessible resources have been developed by those organisations with a particular responsibility for educating about Internet safety. These resources aim to demystify what seems like complex technologies.

It is important to teach children how to use the Internet safely from as early an age as possible. One interactive resource is Netty's World which has been developed by NetAlert. Parents can sign a registration form to enable their children to join Netty's Club.

Netty's World

The Internet offers a range of opportunities for children, but there are also potential dangers of which parents need to be aware.

Netty's World is designed for young children starting out on the Internet. It provides an interactive and safe environment for children to play in, while providing important messages about Internet safety.

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

Source: http://www.nettysworld.com.au/

In addition to Netty's World other interactive resources for students include Cybersmart kids online: smart Net surfing for kids and their grownups, Australian Broadcasting Authority.
http://www.cybersmartkids.com.au

The World Wide Web

Visiting websites is the most common activity students undertake on the Internet. Many children and adolescents accessing the Internet using a computer or another enabled device will 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. These include State-wide Wide Area Networks (WANs), filtering services and moderated search engines.

The Victorian Education Channel

The Victorian Education Channel is an online service provided by the Department of Education and Training in Victoria. The Channel operates as a discovery site for information and services related to education and training that have been produced by the Department and selected third party providers.

In addition to the Victorian Education Channel, there are a number of safe searching environments for students and teachers. These include:

- **EdNA Online – Education Network Australia** http://www.edna.edu.au/edna/
- **Edulist** (Queensland) http://education.qld.gov.au/tal/curriculum_exchange/.

Web authoring

Many students 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. There are a number of Australian guidelines that provide clear advice about web authoring by students. These address issues such as privacy and personal security.

Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'web authoring'.

Online publishing is also governed by State and Territory or Australian statute in areas such as defamation, equal opportunity and racial vilification. These are areas about which students need to be made aware.

Publishing student photographs on the web

Education Queensland publishes guidelines about publishing photographs on the web.

Publication of private information or photographs

Schools should analyse risks associated with posting information about teachers, students or their family on the Internet and develop policies in consultation with their school community. In order to protect the student, considerations might include:

- reasons for the publication, for example outstanding achievements
- student situation, for example age, family situation
- identification of the students, for example publishing first names only, publishing group rather than individual photographs
- ability of others to digitally enhance published medium.

A school's policy might include:

- obtaining parental/guardian permission on a student consent form if details of students, including photographs, are to be published
- publishing the first name only on photographs unless approved by the parent or guardian
- involving students over a particular age in giving approval for having their details and/or photographs published.

Source: Education Queensland website http://education.qld.gov.au/publication/procedure/web/schools/riskman.html

Chat

Chat is a way of communicating with people at the same time by typing messages which then appear on your computer screen, and are sent across the Internet to be read by everyone else 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 and more popular.

The anonymity of participants may lead students to engage in unsafe behaviour, or in other cases to become susceptible to 'online grooming', where an adult takes on the persona of a child in order to befriend a child in a chatroom, ususally with the intention of meeting them in real life. Students need to be careful about how much personal information they give out to the people with whom they are chatting.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'chat rooms'.

Safe Internet chat rooms

The Netlearners section of the Discover website provides a service for Tasmanian teachers where they can use chat safely and securely with their students.

How to host a forum or Internet chat

If you are confident in using forums and chats, you may apply by completing an electronic form to:

- host a forum
- manage an Internet chat.

The Discover Team will set up forums or chats on receipt of these forms and delegate management of them to the teachers who have requested them.

Forums or chats may be requested by teachers for a variety of purposes. Many forums are established as professional development activities to enable teachers to discuss issues of interest. Forums have also been used extensively as part of collaborative projects, enabling students in different schools and classes to share experiences and opinions. To use chat effectively there are some technical/software requirements that can be very easily installed on your computer.

Discover offers a range of forum tools and a choice of text based, comic or virtual reality chat facilities. On receipt of your application to host a forum or manage a chat, you will be contacted to discuss specific customisation to suit the users you have in mind.

Source: http://www.discover.tased.edu.au/netlearn/

In addition to this general Tasmanian resource, the Discover website also offers the following specific resource for LOTE students.
http://www.discover.tased.edu.au/lote/chats/stuchat.htm

An example of another State's moderated chat rooms is provided by the Department of Education and Training, New South Wales.
NSW Web services for schools and TAFE
http://www.det.nsw.edu.au/strat_direction/strat_init/isp/chat/index.htm

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. Instant messaging is also called IM, Iming, Internet Relay Chat (IRC), or ICQ ('I seek you').

Using instant messaging programs exposes students to a number of risks. Private conversations are easy to start with anybody and real time conversations can occur with strangers: personal information may be inadvertently released.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'instant messaging'.

Peer-to-peer (P2P) networking

Peer-to-peer networking programs (P2P) are applications that run on personal computers with the intent to share files with users across the Internet.

P2P networks work by connecting individual computers, forming file sharing communities. Members of the community (those people who have installed the P2P application on their computers) 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, and 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.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'P2P'.

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. Email is great for communication with people and documents, images, text, music and movies can be attached to them. The risks with email include spamming, flaming (attacking someone through email), bombing (sending hundreds of emails to a person to overload their system), stalking, viruses, bullying and inappropriate content.

> Need more help? ☎ 1800 880 176 or go to http://www.netalert.net.au and search for 'email'.

Global Classroom Project

Education Department approved collaborative projects are a focused, moderated means of teaching about the Internet in safe and secure educational environments. By participating in collaborative projects, primary and secondary students can experience and learn about electronic communication, web authoring and a range of other Internet related skills.

The Global Classroom Project is now into its eighth year. During this time, thousands of schools from Australia and around the world have participated in the range of online collaborative projects the Global Classroom has to offer. Schools from as far away as Argentina, Sweden, France and Latvia (to mention just a few) have collaborated and contributed to the teaching and learning activities taking place in Victorian classrooms.

The Global Classroom Project offers teachers:

- access to online collaborative projects covering all year levels, curriculum levels and skill levels
- opportunity to post their own project on the database
- opportunity to place an 'ad' seeking partner schools
- access to teaching and learning resources.

Source: http://www.sofweb.vic.edu.au/gc/

Teaching strategies for Internet safety

A range of strategies can be used by teachers to minimise the risks associated with accessing the Internet using a computer or another enabled device, and instead develop in students an understanding of safe and responsible action.

The skills and knowledge described below, and in the CyberSafe Schools Quick Reference Guide (see page 16) are only indicative. Some students will be more advanced in their knowledge and skills than others and consequently there may be significant gaps in an individual's or group's knowledge and experience.

Internet basics

To navigate a virtual environment safely, and to recognise the different elements of online material, students require a basic knowledge of Internet terminology and functions. In order to teach students such capacities teachers can:

* show students how to distinguish online from offline content
* explain the different functions of browser buttons
* point out the different features of a web page or website
* demonstrate how links work, and the role of graphics and text in communicating information.

Resource discovery

The World Wide Web is a rich source of information and therefore a useful tool for learning, however information found on the web can vary in terms of appropriateness, quality and accuracy.

Safe zones can protect students from exposure to inappropriate material. While technological measures – such as spam filters, content filters and Internet rating systems – are very effective, they are not fail-safe. Consequently students need to be equipped with the skills and knowledge that enable them to deal with exposure to inappropriate material.

Students need to develop safe and effective resource discovery skills. These include skills that enable students to discover and retrieve reliable and relevant information, as well as to discern and deal with inappropriate content.

At a lower primary level

* Identify reliable websites for students to explore.
* Ensure that students use approved, educational search engines.
* Explain and demonstrate techniques of searching using selected keywords.
* Assist students to browse a website to distinguish relevant from irrelevant material.
* Use approved safety procedures for dealing with inappropriate content such as using the back button, exiting the browser, clicking home or turning off the monitor.

As students progress through the stages of schooling, they need to become 'information literate'.

At a middle primary level

* Investigate if the school uses filtering technologies and/or provides access to safe search environments.
* Prepare students to make judgements about the credibility of Internet content based on knowledge of author, publisher and domain extension, for example com.au, edu.au, org.au, gov.au.
* Discuss and explain the importance of safe search engines with students, and model how to use them.
* Use reporting and support protocols for dealing with confronting or unsuitable content.

When students reach secondary school they need more scope to explore the Internet and develop skills that enable them to critically evaluate website content.

At a secondary level

- Encourage exploration of a range of safe and vetted websites.
- Demonstrate how to critically evaluate websites that are sexually exploitative or use racial vilification, or have extreme political views.
- Provide guidance and procedures for dealing safely with confronting or dangerous content.

Personal information and privacy

While identity information can be used for legitimate purposes, it can also be used for dishonest purposes. A general rule is that just as you would not provide such information to someone you meet on the street, nor 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 students, however there is the danger that students will post photographs of themselves or other students to websites. It is also conceivable that a student's email address could be placed on a website, and they could, as a consequence, receive sexually explicit or offensive emails. Placing home addresses and other personal details carry a risk of being used inappropriately.

At a primary level

- Discuss the benefits and risks of personal web publishing.
- Explain school policy in language that is age and capacity appropriate.
- Encourage students to develop web pages that conform to school policy.
- Provide models of safe student web pages.

At a secondary level

- Alert students to the dangers of posting inappropriate content such as sexist, violent or hateful materials.
- Explain that electronic communication should not be used to harass or bully others.
- Explain the dangers of posting identity information.

Students could be confronted with websites that ask for personal information in the shape of online forms. Both risks and benefits associated with revealing identity details could be demonstrated to students.

At a secondary level

- Stress that some websites ask for personal identity information for illegitimate reasons.
- Advise students to generally avoid completing online forms that ask for identity details, and/or to seek advice from teachers or parents if it seems to be a reputable company or organisation.
- Encourage students to seek advice from a teacher, parent or carer if they are not sure about the credibility of the organisation and the information sought.

Communication and collaboration

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 Assistants (PDAs) can also be used for text messaging and for exchanging photographs or video.

There are, however, some risks associated with using these technologies. Emails can contain virus-infected attachments or be used to bully and harass. This may take the form 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.

Students should be made aware of the expectation of the school and their community regarding their own use of email.

- Familiarise students with the school's acceptable use policy.
- Explain that it is not acceptable to send email that makes others feel uncomfortable or that is defamatory.
- Teach the conventions of 'netiquette' for using email. (The NetAlert website contains useful articles on netiquette.)

Students need to know how to deal with email bullying and harassment, and the effect it can have on recipients.

- Advise students to notify a teacher, parent or carer if the sender is a known bully, or if they have sent unpleasant or annoying messages before.
- Ask students to report it to the sender's email account provider – you can find this address after the @ sign – if the bullying happens through a personal email account.
- Instruct students not to open the email if the sender's name is not familiar.
- Look at the message and talk to the student about the issues, emphasising that it is not the student's fault.
- Deal with all instances of bullying in the context of the school's Internet or bullying policy.

Students need to be familiar with appropriate chat room behaviours and the protocols that govern them.

- Emphasise 'stranger danger'. Stress that the people students may meet in chat rooms may not be whom they seem, and that they may imitate the language of students ('online grooming').
- Teach chat protocols in monitored or moderated chat rooms.
- Promote netiquette focused on being polite and considerate.
- Emphasise the importance of not exchanging personal information or photographs of themselves.
- Warn students not to meet someone from a chat room face-to-face unless in the company of an adult in a public place.

Commercialism

The Internet offers many benefits for online commerce, or e-business. It enables people to buy and sell goods and to make financial transactions online. For those setting up a business it offers an additional competitive dimension, however some transactional websites are not what they purport to be. There are illegitimate websites that make false and misleading claims – websites that aim to deceive. Some sites are even bogus or 'dummies'. As a result, transactional websites that ask for credit card details should be treated with caution. Students need to be familiar with personal financial security on the Internet.

- Encourage students to exercise care when making Internet purchases.
- Advise students to ignore unsolicited email, or spam, that makes monetary offers and proposes 'get rich quick schemes'.
- Explain that there are both secured and unsecured websites.
- Demonstrate how to distinguish between secure and unsecured websites.

Bridging the gap between home and school

Schools are relatively confined areas where students can use different technologies under the supervision of teachers or the protection of technologies such as Internet filters. At home, however, the level of protection may not be as high. Technological devices may not be as effective, or they might not even exist.

Parents may be unable to supervise or monitor their children's use of the Internet as effectively as teachers. For example, whereas school codes of conduct and student agreements regulate use of electronic communication, these will not apply at home. Students may deliberately or inadvertently search for inappropriate content at home where they have access to conventional search engines rather than the safe educational websites that they may be required to use at school.

Consequently, it is important that students be taught safe and responsible use of the Internet and be educated about the risks associated with it. The aim should be to equip students with a level of skill and knowledge that enables them to use the Internet safely at all times and in any environment. Schools may choose to advise parents of relevant technologies, guidelines or strategies on using the Internet safely in the home.

Internet safety and the curriculum

The Australian Government Department of Education, Science and Training; State and Territory Education Departments; the National Catholic Education Commission; and the Independent Schools Council of Australia advise that teaching Internet safety skills is an important component of the curriculum. They are unanimous that it is the responsibility of all teachers, rather than teachers in a few subject disciplines.

Most State and Territory curriculums do not refer to Internet safety specifically, although some of the newer syllabuses such as the Queensland Health and Physical Education syllabus now include Internet safety within the Safety strand. While most States and Territories have a Safety strand or its equivalent in their Health and Physical Education frameworks or syllabuses, these make detailed reference to topics such as Traffic safety and Personal security rather than to Internet safety. The connections between these are self-evident, so this learning area may be a useful area to embed teaching about safe use of the Internet.

English curriculums and syllabuses emphasise the development of critical or information literacies. The skills required to evaluate texts are equally applicable to multimodal technologies and to the Internet. Teaching about reading and writing is a core component of most frameworks and syllabuses. Safe student communication and online publishing can be developed in English classes.

Teachers of the Technology learning area, where there is an Information strand or its equivalent, are likely to be high-level users of ICT and online resources. Issues such as the legal, ethical, economic and social impact of the Internet as they relate to Internet safety can be investigated in the Technology classroom.

Many teachers use the Internet for research in learning areas such as English, Languages Other Than English, Science, and Studies of Society and Environment. Teaching about Internet safety within the context of teaching programs in these learning areas is essential if students are to make full and informed use of the Internet as a rich source for learning.

NetAlert
CyberSafe Schools
Quick Reference Guide
Primary

Australian Government

NetAlert Limited

This Quick Reference Guide has been developed for primary teachers. It summarises the more detailed content of the CyberSafe Schools Wall Chart, which was distributed to all schools with this guide. The guide describes:

• the **knowledge and skills** required of students when using the Internet via computers or other enabled devices

• **Internet safety issues** or situations that students may encounter

• **teaching strategies** for Internet safety.

	Knowledge and skills	Internet safety issues	Teaching strategies
Upper primary	Use search engines to effectively locate information. Navigate, browse and retrieve information from websites. Compare and contrast content from similar sources	Resources discovered through Internet searches may contain or lead students to content that is inaccurate, violent, dangerous, sexually explicit or racist.	Development of information literacy to empower students to safely search, navigate and retrieve content, and compare sources for their accuracy, reliability or soundness
	Produce text, images and other elements for publication and communication in a range of contexts	In certain circumstances, students may produce or communicate content that is untruthful, defamatory, or that contravenes school or community standards.	Analysis of personal, school and community standards for interaction and communication to apply when using a range of software for web authoring, email, chat and discussion groups
	Apply basic principles of safe and responsible use of the Internet **At these levels, in addition to skills acquired at lower levels, students will typically:**	Students may be exposed to a range of Internet resources, such as online marketing and advertising, which may be exploitative.	Investigation of Internet commercialism and the social and ethical aspects of these for students
Middle primary	Identify and use terms in searches to discover and retrieve content from a range of online and offline sources	Students may inadvertently come across resources that are confronting, unsuitable or which make them feel uncomfortable.	Guidance for effective resource discovery and basic strategies for dealing with inappropriate or dangerous content
	Use software to edit, format, adapt and generate content for a specific purpose and to communicate with others	Access to communication technologies may result in students receiving abusive and harassing messages with which they are unable to cope.	Modelling and role playing safe responses to harassment and bullying when using particular technologies such as email and chat
	Understand codes of conduct when accessing the Internet **At these levels, in addition to skills acquired at lower levels, students will typically:**	Online publication of personal information or images may result in these being misused by others, or in the student becoming the recipient of sexually explicit or offensive messages.	Establishment of class protocols for online activity that is consistent with school policy. Exploration of a range of scenarios that illustrate safe Internet communication
Lower primary	Recognise that the Internet is a rich source of information and entertainment	Students may access online and/or interactive content that is age inappropriate, graphically confronting or violent.	Provision of a range of online or offline content that is age appropriate, relevant, entertaining and safe
	Understand and use basic terms relevant to the Internet **At these levels, students will typically:**	Students may navigate to inappropriate or dangerous websites using colourful images and icons or by randomly following hyperlinks.	Explanation of the conventions of the online content such as the components of a web page, and navigation within and from a website

NetAlert
CyberSafe Schools
Quick Reference Guide
Secondary

Australian Government
NetAlert Limited

This Quick Reference Guide has been developed for secondary teachers. It summarises the more detailed content of the CyberSafe Schools Wall Chart, which was distributed to all schools with this guide. The guide describes:

- the **knowledge and skills** required of students when using the Internet via computers or other enabled devices
- **Internet safety issues** or situations that students may encounter
- **teaching strategies** for Internet safety.

	Knowledge and skills	Internet safety issues	Teaching strategies
Upper secondary	Employ a range of sophisticated research procedures for online learning. Validate content using credible, external sources	Specific websites target young people and attempt to improperly manipulate their views for racist or extremist purposes, or to recruit students to racist or extremist organisations.	Investigation of a range of sites within subject disciplines to teach high level critical literacy skills that enable students to independently evaluate the quality of sources
	Analyse and structure content to produce complex representations. Communicate these across a range of environments and contexts	As students develop complex personal identities they may engage in unsafe behaviour, using a range of Internet enabled technologies.	Analysis of how chat rooms, ICQ or electronic conferencing operate, and the ways in which the technology may expose students to unsafe activity with peers or adults
	Understand the benefits, constraints and influence of social, legal, economic and ethical issues on use of the Internet and enabled devices **At these levels, in addition to skills acquired at lower levels, students will typically:**	The expansion of e-commerce has both advantages and disadvantages. Students need the knowledge and skills to use online transactions safely.	Investigation of Internet commerce and the technologies used for safe and secure transactions when buying or selling online
Middle secondary	Select appropriate search engines to discover content. Make judgements between search results in order to reach relevant and appropriate content	In schools, students use approved search engines under supervision. They need to develop safe techniques for unsupervised searching across a range of environments and contexts.	Development of information literacy that enables students to safely search, navigate and retrieve content and make judgements about the credibility or quality of resources
	Use a diverse range of communication technologies for educational or other purposes across a range of environments and contexts	Communicating with others using the Internet by computer or another enabled device may expose students to harassment and bullying by peers or adults.	Strategies for dealing with harassment and bullying including procedures and support structures available. Individual responsibilities when communicating with others
	Understand the social, legal, economic and ethical consequences of accessing the Internet by computer or another enabled device **At these levels, in addition to skills acquired at lower levels, students will typically:**	Accessing the Internet by computer or another enabled device to communicate is widespread and students need to become aware of their social, legal, economic and ethical use.	Investigation of the social, legal, economic and ethical use of Internet enabled devices such as mobile and camera phones to text message or exchange photographs or video
Lower secondary	Develop questions or keyword combinations and select appropriate sourcing tools to locate content. Appraise located information	Searching for and finding online content that is inappropriate, such as sexually explicit, violent, or illegal information and images, may be unsafe for students.	Safe and reliable strategies for discovering content using search engines, directories, and links to external resources from within websites
	Synthesise content from a range of sources. Structure, link and present content. Communicate with others for varied purposes in a variety of contexts	Without safe opportunities to collaborate and communicate with peers, students may not acquire the skills to structure, present and communicate safely.	Participation in endorsed collaborative projects where online communication using web authoring, email and electronic conferencing can be learned in moderated environments
	Understand the necessity for laws, codes of conduct and procedures. Recognise the potential for misuse of the Internet and the procedures to address this **At these levels, in addition to skills acquired at primary levels, students will typically:**	Students may inadvertently or intentionally access or publish content or opinion that disregards school codes of practice, or that is unlawful.	Explanation of purpose and application of school policy and procedures in the context of the law. Teaching of Internet safety procedures that are transferable to a range of contexts

Glossary

Acceptable user policy

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

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.

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.

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.

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.

Peer-to-peer (P2P) networking

Peer-to-peer 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.

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.

Stranger danger

Stranger danger is the term used to describe 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.

> For additional advice about these and other Internet safety terms, use the NetAlert Advice Centre.
> http://www.netalert.net.au/00002-Advice-Centre.asp

Resources

Australian Government, State and Territory and sectoral advice

Acceptable use policy for computer facilities and external networks, Department of Education, Employment and Training; Northern Territory
http://www.latis.net.au/resources/index.htm

Child safety on the Internet for teachers and school communities, Department of Education; Tasmania
http://www.education.tas.gov.au/0278/issue/992/safe.htm

Cyber-racism: racial hatred on the Internet, Human Rights & Equal Opportunity Commission
http://www.humanrights.gov.au/racial_discrimination/cyberracism/index.html

EduList, Education Queensland
http://education.qld.gov.au/tal/curriculum_exchange/

Guidelines for Internet access, Department of Education and Children's Services; South Australia, 2004
http://www.news.com.au/common/story_page/0,4057,8370577%255E15306,00.html

Management of student access to controversial material on the Internet, Centre for International Research on Communication and Information Technologies 1996
http://www.dest.gov.au/nbeet/publications/pdf/96_13.pdf

Racial discrimination: guide to the law, Human Rights & Equal Opportunity Commission
http://www.humanrights.gov.au/racial_discrimination/guide_law/index.html

SafetyNet: Internet usage: guidelines for schools, Department of Education, Employment and Training; Victoria
http://www.sofweb.vic.edu.au/internet/safety.htm

School Internet services acceptable usage policy, Department of Education and Training; New South Wales 2002
http://www.det.nsw.edu.au

Student safety online, Department of Education and Training; Western Australia
http://www.eddept.wa.edu.au/cmis/eval/curriculum/ict/safety/index.htm

Technology Position Statement, Queensland Catholic Education Commission
http://www.qcec.qld.catholic.edu.au/pdf/QCEC%20-%20Technology%20Position.pdf

Selected teacher and student resources

Cybersmart kids online: smart Net surfing for kids and their grownups
Australian Broadcasting Authority, Sydney
http://www.cybersmartkids.com.au/

CyberNetiquette Comix, Disney Online
http://disney.go.com/cybersafety/

NetAlert: Australia's Internet Safety Advisory Body Advice Centre
http://www.netalert.net.au/00002-Advice-Centre.asp

The NetAlert Advice Centre offers solutions to Internet safety issues. In the advice centre you can find:

- a toll free Helpline to answer questions about Internet safety

- monthly enewsletters filled with practical advice and solutions on Internet safety

- downloads including information sheets, user guides, online reports and Internet safety materials

- a Safety Solution Finder where users may browse topics or ask questions online

- directories of Internet safety resources.

Netsmartz Workshop [United States]: National Center for Missing & Exploited Children.
http://www.netsmartz.org/

Netty's World
http://www.nettysworld.com.au/

Netty's World is designed to educate young children on how to use the Internet safely. Netty's World provides an interactive and safe environment for children to play in, while providing important messages about Internet safety.

Parents sign the registration form to allow their children to join Netty's Club.

NetAlert encourages adults to take young children through the online storybook, 'Netty's Net Adventure' where important Internet safety messages are explained. Children are encouraged to play the interactive games where the Internet safety messages are reinforced.

CyberSmart! curriculum [United States]
http://www.cybersmartcurriculum.org/

i-SAFE America [United States]
http://www.isafe.org/

Kidsmart [United Kingdom]
http://www.kidsmart.org.uk/

The Cyber Citizen Partnership [United States]
http://www.cybercitizenship.org/