Cybersmart Guide for Library Staff
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>How to use this guide</td>
<td>4</td>
</tr>
<tr>
<td>Using this resource in the library</td>
<td>5</td>
</tr>
<tr>
<td>Support for internet-use policies</td>
<td>5</td>
</tr>
<tr>
<td>Introducing the guide in your library</td>
<td>5</td>
</tr>
<tr>
<td>Online activities at the library</td>
<td>7</td>
</tr>
<tr>
<td>Supporting library users—specific issues</td>
<td>8</td>
</tr>
<tr>
<td>Exposure to inappropriate material</td>
<td>8</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>9</td>
</tr>
<tr>
<td>Privacy and private information</td>
<td>10</td>
</tr>
<tr>
<td>Spam</td>
<td>10</td>
</tr>
<tr>
<td>Unreliable information</td>
<td>11</td>
</tr>
<tr>
<td>Scams</td>
<td>12</td>
</tr>
<tr>
<td>Supporting library users—managing risks</td>
<td>13</td>
</tr>
<tr>
<td>Chat</td>
<td>13</td>
</tr>
<tr>
<td>Instant messaging</td>
<td>13</td>
</tr>
<tr>
<td>Social networking</td>
<td>13</td>
</tr>
<tr>
<td>Online games and virtual communities</td>
<td>14</td>
</tr>
<tr>
<td>Pop-ups</td>
<td>15</td>
</tr>
<tr>
<td>Support services</td>
<td>16</td>
</tr>
<tr>
<td>Practical solutions</td>
<td>16</td>
</tr>
<tr>
<td>Report a crime</td>
<td>16</td>
</tr>
<tr>
<td>Talk to someone</td>
<td>16</td>
</tr>
<tr>
<td>Cyber rules for young library users</td>
<td>17</td>
</tr>
<tr>
<td>A summary of strategies to support safety online</td>
<td>18</td>
</tr>
<tr>
<td>Internet basics</td>
<td>18</td>
</tr>
<tr>
<td>Children and the internet</td>
<td>18</td>
</tr>
<tr>
<td>Education</td>
<td>18</td>
</tr>
<tr>
<td>Reporting or making a complaint</td>
<td>18</td>
</tr>
<tr>
<td>Networking with other libraries</td>
<td>18</td>
</tr>
<tr>
<td>Glossary</td>
<td>19</td>
</tr>
<tr>
<td>Other useful links</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

The Cybersmart Guide for Library Staff provides information and resources about safe, responsible and enjoyable internet use in Australian libraries, including public libraries and school libraries. The guide is intended to both inform and support library staff in promoting safe internet use in the library environment—particularly to children.

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

The ACMA is responsible for the regulation of broadcasting, the internet, radiocommunications and telecommunications. The ACMA’s responsibilities include:

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

For library staff, the ACMA’s cybersafety program includes web-based and printed materials on internet safety. All materials for library staff are available online at www.cybersmart.gov.au.

The ACMA worked closely with the Australian Library and Information Association and Australian libraries to ensure that all materials are both accurate and appropriate. Recognising that most Australian libraries have internet-use policies, this guide aims to complement existing policies and provide additional resources and support to library staff.

For more information or advice on internet safety visit the Cybersmart website www.cybersmart.gov.au or contact the ACMA’s Cybersafety Contact Centre on 1800 880 176.
How to use this guide

This Cybersmart Guide for Library Staff is a resource developed by the ACMA to provide library staff with the information, support and tools to effectively promote internet safety in Australian libraries. This guide is complemented by information for families, in the Cybersmart Guide for Families, a cyber rules poster for young internet users and a series of cybersafety online videos. Together these materials aim to inform and support library staff, who can then better assist internet users, particularly young users, to have positive internet experiences.

Information in this guide is set out in the following sections for easy reference.

Online activities at the library

This section provides an overview of the benefits in using the internet, including a summary of activities that young library users engage in online and an overview of the issues they may face.

Supporting library users

This section looks at risks and issues in greater detail. It offers library staff valuable information about ways they can support library users in addressing particular situations.

Support services

Sometimes, library users may seek specific internet safety guidance. They may require expert advice or referral to an internet safety organisation. This section links libraries with the range of Australian services and reporting mechanisms for common internet safety complaints and issues.

Copies of this and other library program materials are available at: www.cybersmart.gov.au
Informing library staff about cybersafety is an important step towards better educating young internet users. This guide is designed to provide information and contacts which support internet safety activities in a library environment. The guide should complement existing internet-use policies and is able to be used in professional development programs within the library.

Support for internet-use policies

Most libraries have implemented internet-use policies and publicise these policies widely in their communities. These policies cover the terms and conditions for public use of library internet access terminals, including children's use of the internet.

The Australian Library and Information Association has also developed policy guidelines for use in libraries. This includes guidelines for library internet-use policies and children's use of the internet. These guidelines can be found at: www.alia.org.au.

This Cybersmart Guide for Library Staff is intended to support and complement these existing internet-use policies in libraries and to provide advice on cybersafety.

Introducing the guide in your library

The Cybersmart Guide for Library Staff is relevant to library staff at all levels, from trainees to experienced library managers who wish to know more about internet safety. It aims to provide general information as well as specific details on how to respond to issues as they arise.

One suggested approach to communicating with library staff on internet safety is to:

» identify a ‘champion’ or a team within the library with an interest in, or responsibility for, internet safety

» review the ACMA cybersafety material either in print form or from www.cybersmart.gov.au

» include this guide in new staff induction programs

» introduce this guide and the Cybersmart Guide for Families at a staff meeting. Suggest how staff may use them. Refer to the Cybersmart website

» identify procedures to action activities suggested in this guide

» evaluate, update and publicise the library’s internet-use policies and practices

» post specific support services in user guides at the front desk and on the intranet, if applicable

» communicate and use internet safety resources with library users. For example, display the cyber rules poster at the internet access terminals within or in the children’s area of a public library. Make the Cybersmart Guide for Families available.

Additional materials

Additional copies of Cybersmart Guide for Library Staff, Cybersmart Guide for Families and the cyber rules poster can be ordered by contacting the Cybersafety Contact Centre on telephone: 1800 880 176 or email cybersmart@acma.gov.au.

All materials are available free of charge.

Library staff may like to link to the library materials on the Cybersmart website through their library’s intranet, if applicable. Visit: www.cybersmart.gov.au
The internet has become an integral part of life. It enables people of all ages to learn and communicate in a myriad of new ways. For children, growing up in a world where the internet has always been available, it is an essential tool. They are the ‘digital natives’—always surrounded by online technology, and using the internet from an increasingly early age.

The internet is a powerful resource, both for learning and communication. In a library environment, the internet can provide many benefits for young library users, including developing:

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

People learn by being able to find relevant and reliable information quickly and easily, and being able to select, interpret and evaluate that information. Searching for information on the internet can help develop these skills. Since many sites present particular viewpoints, the internet is a useful mechanism for learning to distinguish fact from opinion.

Libraries provide access to online resources and services play an important role in ensuring that communities who do not have access to these services at home are not disadvantaged.

Despite educational and social benefits of information and communication technologies, there are risks associated with their use, particularly for young library users of school age.

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

» giving out personal details about themselves to people or organisations they don’t know
» posting unsuitable information online, including photos
» agreeing to meet people they’ve only ever met online, without speaking to a parent or carer
» using provocative pseudonyms
» sharing passwords
» posting public profiles about themselves
» unsafe browsing or searching, clicking on links that take them to unsuitable web pages
» opening messages from people they don’t know
» responding to nasty or suggestive messages
» using online games or virtual worlds that are only for people over 18
» accessing inappropriate or illegal material.

Not all library users will experience problems. Empowering young users will help them to have safe and positive internet experiences.
Guidance about specific online issues will help young library users to minimise risks and enjoy positive internet experiences. The issues include:

**Exposure to inappropriate material**

Young internet users may face exposure to material that is inappropriate for them. This may be because it is sexually explicit, offensive or violent, or material that encourages dangerous or illegal activities. Some sites promote extreme political, violent, racist or sexist views. This material can be accessed through website browsing, through newsgroups, shared in peer-to-peer networks, or sent by email or instant messaging services.

Inappropriate material can be accessed inadvertently, when searching for educational content about people, places or issues, or it may be intentional.

**Notes for library staff**

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

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

- detailed instruction in crime, violence or drug use
- child pornography
- bestiality
- excessive violence or sexual violence
- material that advocates committing a terrorist act
- actual sexual activity.

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

The ACMA can investigate complaints made about:

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

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

If the content is sufficiently serious, for example, illegal material such as child pornography, the ACMA will refer the content to the appropriate law enforcement agency for criminal investigation.

For more information on the ACMA's role in regulating online content go to: www.acma.gov.au/hotline.
Library staff can:
» provide library users with information on safe searching techniques
» provide information to library users on how to deal with inappropriate material
» remind users that the internet should not be used to access inappropriate or illegal material
» assist library users to report to the ACMA any material suspected of being prohibited
» make a list of safe websites available for young library users to visit, and provide links to websites for children and young people that contain material especially for them
» offer internet training sessions
» add internet use policies as part of the login procedure for everyone accessing library computers.

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

Cyberbullying includes teasing, spreading online rumours and sending unwanted or threatening messages or defamatory material. While it can have a damaging effect on young people, there are practical steps they can take to retain control of the situation.

Notes for library staff
Bullying can lead to serious emotional and behavioural problems in young people. To help young people address these issues, a number of support services are available:

» Kids Helpline: www.kidshelp.com.au
   Telephone: 1800 551 800
» Bullying No Way: www.bullyingnoway.com.au

Library staff can:
» offer internet safety sessions for library users
» provide library users with links to cyberbullying advice and information
» provide library users with information on available support services such as the Kids Helpline or the Bullying No Way website.
Privacy and private information

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

Providing personal information online can result in a user being the target of spam, advertising materials and/or viruses. In some cases websites prompt users to reveal private information on forms. Not all these requests are legitimate.

Young library users need to understand that they should ask a parent or carer before they give anyone on the internet their personal details. Once information is posted online it is very difficult to remove.

Notes for library staff

Advise library users to contact, or ask their parents to contact, the author or website administrator if a website contains personal details that have been disclosed without authorisation. Website administrator details are commonly located on website home pages. A lawyer may also be able to provide assistance.

If a library user reports that their personal details have been mishandled by a Commonwealth Government agency, or a private sector organisation, they should be referred to the Office of the Federal Privacy Commissioner.

For more information go to: www.privacy.gov.au.

If a library user is concerned that disclosure of their personal details has put them at risk, they should contact their local police station.

Library staff can:

» offer internet training sessions for library users
» advise library users to establish a separate web-based mail account for certain online activities, such as subscription sites or social networking accounts
» provide library users with links to information about privacy and how to report privacy complaints.

Spam

Any library user, including young people with a personal email address or mobile phone, can receive unwanted messages. These are called spam. Spam messages may be inappropriate, offensive, or contain computer viruses. They frequently promote products or services, but can simply be a message claiming to be from a ‘secret admirer’ or friend. Responding to these messages can lead to further unwanted spam, often at considerable cost to the user if the spam is sent via mobile phone.

There are some simple safety rules to combat spam—don’t click on any link in an email, and don’t respond in any way to unknown or secret admirer type messages.
Notes for library staff

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

While the Act relates to commercial messages, a message may not necessarily appear to be commercial. One example is a message claiming to come from a ‘secret admirer’ or friend where, if a person fills in their mobile telephone number, they are then sent high-cost premium mobile messages.

Spam complaints should be directed to the ACMA. The ACMA can take action against spam sent from within Australia. To make a complaint, complete the online form at: www.acma.gov.au/spam.

The ACMA has a number of tools available to report spam including the SpamMATTERS reporting button which home users can download. See how to download and use SpamMATTERS at www.spam.acma.gov.au. The ACMA also has an extensive frequently asked questions section about spam which can also be accessed from this link.

Unreliable information

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

Library users need to be able to distinguish fact from fiction online and learn the basics about copyright. Young people also need to develop good browsing and searching skills to ensure they visit safe areas and find appropriate information. Library staff can play an important role in fostering these skills.

Library staff can:

- provide library users with a list of good websites to visit and information on safe searching techniques
- provide library users with information on how to evaluate websites for accuracy and authenticity
- make a list of safe websites available for young library users to visit, and provide links to websites for children and young people that contain material especially for them
- offer training sessions in effective internet searching.
Scams

Internet scams play on innocent users. Even for young users, there are ways to tell scams from legitimate offers—and places to lodge a complaint and seek advice if a user feels they’ve been scammed.

Scammers use the internet in a number of ways, including:

» promoting fraud via email
» promoting free offers and pyramid schemes through websites
» creating fraudulent advertising materials that are displayed when searching the internet.

Young library users need to understand that if something seems too good to be true, it probably is.

Notes for library staff

If a library user has received a spam email from an Australian business that attempts to facilitate online fraud it can be reported to the relevant consumer affairs or fair trading body in each state or territory.

If a library user reports they are a victim of online fraud or have come across what they suspect to be an online fraud or scam they can report it to the Australian Competition and Consumer Commission’s ScamWatch website at www.scamwatch.gov.au or telephone 1300 302 502.

Library staff can:

» provide library users with information on how to recognise scams and report suspected scams to ScamWatch
» provide library users with information on dealing with pop-ups and other security issues
» create a web page on the library intranet with links and further support for library users
» make a list of good websites available for young library users to visit, and provide links to websites for children and young people that contain material especially for them.
Chat

Chat is a way of communicating in real time with a number of people simultaneously. Users type messages that are sent across the internet to be read by others participating in the chat room. Many chat rooms are unmoderated, so comments are not censored. Chat rooms can be anonymous, so children often talk about things they may not have the confidence to say face-to-face. They can pretend to be someone else—older, smarter or more popular.

Young library users may be tempted to agree to meet an online friend in real life without recognising the risks. In some cases, paedophiles have used chat rooms, email and social networks to gain a child’s confidence and to arrange face-to-face meetings.

Instant messaging

Instant messaging is a form of online chat involving two or more individuals. When a user sends an instant message, it appears on the recipient’s screen almost instantly. Some services also enable files to be sent. Many public library online reference services use instant messaging such as Ask a Librarian and AskNowService.

Like chat, instant messaging can expose users to a number of risks. Private conversations are easy and users can message anyone, at any time. Real-time conversations often occur with complete strangers. While this may be part of the attraction for young users, they can inadvertently share personal information with people with whom they may not otherwise wish to communicate.

Notes for library staff

If a child is suspected to be in immediate danger from contact made via chat or instant messaging, call the police immediately on the triple zero (000) emergency call service number. Concerns about inappropriate behaviour toward children online can be reported to the AFP’s Child Protection Operations Team at www.afp.gov.au/online_form/ocset_form.html.

Library staff can:

- provide library users with information on how to report complaints of suspected child abuse or exploitation
- refer library users to the cyber rules for internet use
- make a list of good websites available for young library users to visit, and provide links to websites for children and young people that contains material especially for them
- offer internet safety training sessions.

Social networking

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

Different social networking sites have different purposes, including to:

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

Notes for library staff

Where offensive or illegal content appears on a social networking website, users can contact the administrators of the website directly to request that the content is removed.

Social networking sites generally have policies about unacceptable content, restricting content that users are allowed to upload. Some sites limit false profiles, content containing nudity or content which presents graphic violence.
Online games and virtual communities

Online gaming sites and virtual communities are particularly popular with young people. They may visit these sites while in a library. Many users have avatars—2D and 3D character representations of themselves—that are able to interact with others. Players can be connected by a worldwide network and can chat, send files, view other players through webcams and publish personal information. Popular online games include RuneScape and World of Warcraft.

Popular virtual communities include Club Penguin and Habbo Hotel.

Library users face the same safety risks on these sites as with other technologies. They should be aware of where to go for help and how to minimise the risks of their use.

Library staff can:

- provide library users with information on how to report abusive or illegal behaviour
- assist library users to report to the ACMA any material suspected of being prohibited
- make a list of good websites available for young library users to visit, and provide links to websites for children and young people that contain material especially for them
- offer internet training sessions
- make internet use policies part of login procedure for everyone accessing library computers.

Website administrators generally rely on complaints from other users to identify unacceptable content, though this can be difficult to monitor because of the large quantities of content posted every day.

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

When making a complaint to the ACMA about content, users should provide the web address and any login details. Login details, such as a user name and password, are particularly important as many social networking sites restrict information to friends or affiliated users.

Complaints about content can be made through an online complaint form, at www.acma.gov.au/hotline.
Pop-ups

Pop-ups are small windows that appear in an internet browser. Pop-ups can appear suddenly for a number of reasons such as when a link or picture on a web page is clicked on or the mouse moves over a hidden trigger. There are some pop-ups that are legitimate and are used for meaningful purposes in some websites. However, some contain inappropriate content or online scams. Spyware pop-ups can transmit personal information. Pop-ups can be difficult to close, cause computers to run slower, and sometimes freeze.

Types of pop-ups include:

» Browser pop-ups—these appear when users are looking at web pages. They often contain advertising or inappropriate content

» Browser pop under—these are windows generated underneath the current web page being viewed that appear after the user starts closing down windows in the foreground

» Messenger Service advertisements—these windows appear like real system messages generated by the computer. They appear when Windows 2000 or XP is being used

» Spyware generated pop-ups—these are created by malicious computer programs or spyware that is installed on the computer.

Notes for library staff

There are ways to prevent pop-ups:

» Install blocking programs—there are many programs that will help to block pop-ups, and many of these are free to download and install. Search for ‘pop-up blockers’ to find one that is suitable for the computer. Pop-up blockers cannot always determine good pop-ups from the annoying ones so users may need to temporarily allow pop-ups to exist on trusted websites

» Download and install a toolbar—toolbars are small programs that attach themselves to the user’s internet browser. There are many toolbars available which have the ability to block pop-ups from appearing in the browser. Some popular toolbars include the Google Toolbar and Yahoo Toolbar. Toolbars are generally free and can be installed quickly and easily

» Configure the computer's browser—a number of popular browsers including Safari, Mozilla and Opera allow users to configure them to block pop-ups. Check the help systems to get started

» Use the keyboard to escape—sometimes users may need to close a window without using the mouse. To do so, press the CTRL and W keys together. This will close down any active windows and is useful for windows that take up the full screen.

Library staff can:

» provide information to library users on how to deal with pop-ups on library internet terminals

» provide information on the risks of entering personal information into pop-up windows.
Access to internet safety support services is important for library staff. Library staff can also provide library users with this information if they have a safety concern or matter to report.

The Cybersafety Contact Centre is a free confidential helpline service. The helpline is available seven days a week from 8:00 am until 10:00 pm on free call 1800 880 176.

There are a range of other agencies that deal with specific internet safety complaints or issues. These include:

**Practical solutions**

**Australian Communications and Media Authority**
For information and advice about online safety issues and to order cybersafety resources
Cybersafety Contact Centre
Tel: 1800 880 176
Visit: www.cybersmart.gov.au
To make a complaint about prohibited online content

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

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

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

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

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

**Report a crime**

**Crime Stoppers**
Tel: 1800 333 000

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

**AFP Child Protection Operations Team**
Report concerns about inappropriate online behaviour toward children

**Talk to someone**

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

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

**Kids Helpline**
Tel: 1800 55 1800
Visit: www.kidshelp.com.au
Cyber rules for young library users

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

» Think before you post information online—once posted it’s difficult to remove.
» Ask your parent/carer before you give anyone on the internet your name, address or any personal details.
» Be careful who you trust online. Making new friends can be fun, but there’s a chance that they may not be who they say they are.
» Always keep your password a secret.
» Set your profile to ‘private’ so your personal information is kept secret.
» Ask a librarian about good sites to visit and about safe searching techniques. Browsing is a great way to find things, but you may not end up where you planned.
» Don’t open messages from people that you don’t know. These could be nasty, contain viruses or be trying to sell you something.
» Tell your parent/carer or the librarian if you are upset by language, pictures or anything scary on the internet.
» Don’t accept any offers that seem too good to be true—they probably are.

This information is reproduced in the cyber rules poster for young library users. Library staff are encouraged to display the poster in the internet area and/or the children’s area of the library.

For more information about the cyber rules go to www.cybersmart.gov.au.
A summary of strategies to support safety online

The following is a summary of the approaches library staff can adopt to encourage young people and their families to use the internet safely and have fun.

**Internet basics**

To navigate a virtual environment safely, and to recognise the different elements of online material, young library users require a basic knowledge of internet terminology and functions.

To assist library users library staff can:

» use the *Cybersafety Guide for Library Staff*, become aware of internet safety advice and communicate this to library staff
» attend a training session or watch the online training videos at www.cybersmart.gov.au
» add internet use policies as part of the login procedure for everyone accessing library computers
» make the *Cybersafety Guide for Families* available in a prominent area, encouraging library users to take a booklet home to read. For additional copies, contact the Cybersafety Contact Centre on 1800 880 176
» create a web page on the library intranet with links and further support for library users
» link your library’s intranet to the ACMA library area at www.cybersmart.gov.au

**Children and the internet**

To assist young library internet users, library staff can provide the following:

» a cyber rules poster in a prominent area of the internet and/or children’s area
» a list of safe websites for children to visit
» information on safe searching techniques
» links to safe sites for children from the library intranet.

**Education**

It’s important that library staff and library users alike are educated in safe and responsible internet use. They can:

» participate in an internet safety training session either in person or online from www.cybersmart.gov.au
» offer internet safety classes for parents, children and other users
» engage with children to create safe site lists
» provide links to internet safety information for library users of all ages.

**Reporting or making a complaint**

If there is an issue, library staff can help to:

» assist library users with internet safety complaints or issues
» refer library users to the appropriate agency or the Cybersafety Contact Centre on toll free 1800 880 176.

**Networking with other libraries**

Talk with other library staff and share ideas for how to address issues in the library.
### Glossary

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

**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 library users can arise with chat room participants pretending to be someone they are not.

**Email**
Email is a service that lets users send a message to another person via the internet. The message is stored on a computer and is read when the recipient checks their mail.

**Filters**
A filter manages access to online content. An internet 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.

**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 young people and adults alike. Some programs allow many people to chat at the same time, like a private chat room.

**Netiquette**
Netiquette is derived form 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.

**Podcasting and vodcasting**
A podcast is a pre-recorded audio program available on the internet and can be downloaded to your computer or MP3 player. A vodcast is the video version.

**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.

**RSS feeds**
RSS stands for ‘really simple syndication’. With an RSS reader, users can scan hundreds of news headlines from one location.

**Search engines**
Search engines are websites that help users to find information on the internet. There are a number of family-friendly search engines which help users find safe websites.

**Social networking**
Social networking describes a variety of services like YouTube, MySpace, Facebook and Twitter. These websites allow users to create profiles, communicate with others and form networks of friends online.

**Tagging or social bookmarking**
Tagging or bookmarking describes the process of assigning a word to a piece of information such as an image, article or video clip that describes the content of the item. Users can search and cross reference information online.

**Virtual worlds**
Virtual worlds are simulated environments created on the internet that people can visit.

**Wikis**
Wikis are online groups of webpages that users can content to and change freely on the internet. The most famous wiki is ‘Wikipedia’.
Other useful links

**Australian Library and Information Association (ALIA)**
Visit: www.alia.org.au

**Australian School Library Association (ASLA)**
Visit: www.asla.org.au
Canberra Office  
Purple Building, Benjamin Offices  
Chan Street, Belconnen  
PO Box 78,  
Belconnen ACT 2616  
Tel: 02 6219 5555  
Fax: 02 6219 5200

Australian Communications and Media Authority

Melbourne Office  
Level 44, Melbourne Central Tower  
360 Elizabeth Street, Melbourne  
PO Box 13112 Law Courts  
Melbourne Vic 8010  
Tel: 03 9963 6800  
Fax: 03 9963 6899  
TTY: 03 9963 6948

Sydney Office  
Level 15, Tower 1 Darling Park  
201 Sussex Street, Sydney  
PO Box Q500  
Queen Victoria Building NSW 1230  
Tel: 02 9334 7700, 1800 226 667  
Fax: 02 9334 7799