



# Internet Access Guidelines for public libraries

Public Libraries Western Australia

July 2017

# Public Libraries Western Australia

Public Libraries Western Australia Inc. (PLWA) was constituted in 2009 to be the peak body to represent public libraries in Western Australia and to work nationally with Public Libraries Australia (PLA) and the Australian Library & Information Association (ALIA).

## Vision

In today's rapidly changing digital world, public libraries are leaders in embracing new technologies to provide interactive public spaces responsive to the technology transformation of our society; community digital hubs for capacity building and connectivity; and greater opportunities for technological literacy and digital transformation. Public libraries play a pivotal role in encouraging library staff and communities to become smart, safe and responsible digital citizens.

Public Libraries Western Australia is pleased to support the eSmart Libraries cyber safety initiative and, in conjunction with the Alannah & Madeline Foundation and the Telstra Foundation, has developed an IT Guidelines Policy to assist WA public libraries in preparing their eSmart documentation.

## eSmart Libraries

eSmart Libraries is a behaviour change initiative for cyber safety and wellbeing designed to equip libraries and connect library users with the skills they need for smart, safe and responsible use of technology.

Being eSmart means knowing how to guard against security and privacy risks online, download content in a legal and ethical way, research and reference information, as well as manage reputation and relationships in cyber space. eSmart helps to embed a culture of positive technology use, create policies and procedures, gain access to evidence-informed resources and track progress in becoming eSmart.

Public Libraries Western Australia is committed to supporting the eSmart Libraries initiative, developed by the Alannah & Madeline Foundation and the Telstra Foundation.

Visit [eSmart Libraries](http://www.esmartlibraries.org.au) for more information.  
([www.esmartlibraries.org.au](http://www.esmartlibraries.org.au))

# Overview

The purpose of this policy is to outline the obligations and responsibilities of all users of the library's public electronic resources. This policy has been developed in order to provide smart, safe and responsible use of technology within the library.

## Scope

This policy applies to all users of the library's facilities and public electronic resources. These facilities and resources include but are not limited to computer and internet access, scanning and printing services and use of online databases.

## Definitions

- Cyber safety - refers to the safe use of Information and Communication Technologies (ICT) equipment or devices (including cellular phones) and the internet
- Cyber bullying – refers to the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature
- eResources – electronic resources such as databases and exclusive online content
- Fixed computer access – individual stationary computer terminals that offer internet access and an Office suite of desktop programs
- Wireless internet - wireless connectivity to the internet on a person's home computer, laptop, smartphone or similar mobile device
- Minors – a person under the age of eighteen years

# Acceptable Use

## Overview

Facilities and resources within the library must be used in an acceptable and lawful manner by all users. Staff will work with the public to ensure compliance with the Policy, Guidelines and Procedures for responsible internet use at all times.

## Principles of Conduct

All users must adhere to the Western Australia Classification (Publications, Films and Computer Games) Enforcement Act 1996, Criminal Code Act 1995, Copyright Act 1968.

# User Responsibility

## Overview

PLWA is committed to providing an environment that is free from harassment, discrimination and bullying. All users of the library are expected to behave in an appropriate manner and respect all other people and facilities within the library. Electronic resources and facilities are expected to be used for the purpose for which they are provided; education and information.

Users are required to comply with the specified rules and procedures to help ensure the legal, safe, and continuing availability and use of these resources.

## Responsibilities

- Refrain from illegal or unethical use of the internet
- Users must perform their own computer activities, however staff assistance is offered subject to availability of staff resources
- Users are responsible for their personal belongings and it is at their own risk to leave any item unattended
- A user is responsible for deleting any of their own files or documents saved to a library computer or device
- Users are responsible for any material they access during an internet session
- Users are responsible for the backup of their own files and documents to their own storage device
- Respect intellectual property rights by making only authorised copies of copyrighted, licensed, or otherwise controlled software or data residing on the internet.

## Behaviour

Users are reminded that the library is a public area which is shared with people of all ages, backgrounds and beliefs. Individuals are expected to consider this diversity and respect the rights of others when accessing potentially offensive information or images. To achieve an atmosphere conducive to the best use of its resources, the following behaviour guidelines are fitting for all users of its in-house electronic resources to abide by:

- Users must be courteous and respectful to all other library users and staff
- Internet access provided by the library must not be used as a medium to bully, harass, threaten or intimidate other users
- Users must listen to and take direction from staff where it is given
- All equipment and resources are to be shared equally
- Staff assistance is offered subject to availability of staff resources
- Users must not seek out, access or send any material of an offensive, obscene, pornographic, threatening, abusive, defamatory or otherwise inappropriate nature
- Users are required to comply with all library policies and State and Commonwealth legislation

## Computer Access

The access and use of library resources and technology are governed by Australian laws. Authorisation to use the library's resources is provided in accordance with these laws. Access rights may be removed if you fail to comply with these laws.

Some activities are unlawful and prohibited. These activities include but are not limited to the following:

- to gain access to any material that is pornographic, offensive or objectionable
- to engage in any conduct that breaks Federal, State or Local Council laws and regulations
- to send or forward any material that is abusive, sexist, racist or otherwise illegal
- to circumvent any filtering or other content access device or software
- for illegal purposes or practices
- for any purpose if the library advised you that such purpose was prohibited
- in any way which damages or interferes (or threatens to damage or interfere) with the operation of the service or with the efficiency of the network.
- to transmit, publish or communicate any material or engage in any conduct which is defamatory, abusive, menacing or harassing
- to engage in abusive behaviour toward staff or other computer users
- to make inappropriate contact with children or minors
- to access, store, reproduce, distribute, publish or commercially exploit any information or material of any kind that infringes any copyright, patent, trade mark, design or other intellectual property right
- to access, monitor, use or control any other person's equipment, systems, networks or data without that person's consent
- to access, or attempt to access, the accounts or private information of others, or to penetrate, or attempt to penetrate, the library's or a third party's security measures, computer software or hardware, electronic communications system or telecommunications system
- to use or distribute software with the intent of compromising network security
- to make fraudulent offers or to advance any type of financial scam
- to engage in any unreasonable activity which impairs the ability of other people or systems to use the libraries services or the internet.

## Copyright Warning

Property rights apply to material accessible throughout the library. It is the user's obligation to operate within the legal system.

- Check for a copyright notice or other information to determine what you can do with the material. If it is not clear that you are allowed to use the material the way you may want to, you must contact the copyright owner before attempting to use it.
- Copyright and other laws apply to most materials on the internet. Copyright owners are entitled to determine who may use and access their materials and on what terms. If you interfere with the owner's rights, legal action may be taken against you.
- Australian laws determine what is a "fair dealing" in copyright materials.

## Content

Libraries do not control the content or layout of any material on any external site. Libraries do not make any representation or warranty about relevancy, accuracy, quality or validity of any material and you must make that judgement for yourself. Some material you access may require you to divulge personal details and credit information: you do so at your own risk.

All use of resources and services is at your own risk.

In the interests of privacy remember to log off the library computer after use.

## Spam

'Spam' includes one or more unsolicited commercial electronic messages with an "Australian link" as contemplated by the Spam Act 2003. You must not use the Service to:

- send, allow to be sent, or assist in the sending of Spam
- relay e-mail from a third party's mail server without permission or which employs similar techniques to hide or obscure the source of the e-mail
- connect to the library network with an open relay mail server or any other device which may allow third parties to use that mail server or device for the purposes of sending electronic messages, solicited or otherwise, with or without their prior knowledge or consent
- use or distribute any software designed to harvest email addresses
- otherwise breach the Spam Act 2003 or any regulations made under the Spam Act 2003.

## Inappropriate Sites

The library has the right to block content that may harm its property and/or network, or content that may distress or upset other users.

Sites that are inappropriate to access include: Adult/Sexually Explicit; Anonymizer; Gore; Hacking; Illegal Activity; Peer-to-Peer; Spam URL's; Spyware.

The definitions of these categories are as follows:

### Adult/sexually explicit

Sites that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. This category includes the following:

- Sex chat rooms
- Sex portals
- Pornography (including magazines, pictures, videos and phone sex)
- Adult services (including escort, stripper, and mistress services)
- Adult personal advertisements

### Anonymizer

Sites that offer anonymous access to web sites, often used to bypass corporate and school proxy controls as well as parental control filtering solutions.

## Gore

Sites that display graphic violence and the infliction of pain or injuries, including the following:

- Gross violence towards humans or animals
- Scenes of dismemberment, torture, massive blood and gore
- Sadism and other types of excessive violence

## Hacking

Sites that promote or provide the means to practice illegal or unauthorized acts of computer crime using technology or computer-programming skills. This category includes:

- Hacker magazines
- Password, software, or other 'cracks' for download or trading
- Sites offering software license keys
- Tools and scripts for hacking

## Illegal activity

Sites with illicit content or instructions for threatening or violating the security of property or privacy of people. This category includes the following:

- Child pornography and paedophilia sites
- Child-oriented erotic sites that are registered with global advocacy groups
- Theft of money, goods and phone services
- Lock-picking and burglary
- Fraud, identity theft, and stealing credit card numbers
- Telephone crime
- Evading or circumventing the law

## Spam URL's

Website URL's found in spam email

## Spyware

Sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, the end user or organization, including the following:

- Sites that carry malicious executables or viruses
- Third-party monitoring
- Malware with 'phone home' destinations

## Wireless Internet

You must use reasonable endeavours to secure any device or network within your control against being used in breach of the internet. The library does not guarantee access to any internet site. The library reserves the right to restrict access to certain types of files and download sizes.

Filtering on the library's wireless internet is dependent on the provider of the service. The library assumes no responsibility or liability for any damage caused to hardware or software due to electrical surges, equipment malfunction, security issues, hacking or viruses.

## Web Privacy

### Monitoring

The library reserves the right to monitor and inspect without consent any data on a library computer system. Such inspections will occur to prevent, detect and minimise the unacceptable usage of the computer system.

## Cyber Safety

The library has a responsibility to provide a safe environment to the general public that promotes respect and equality of all members of the community. Where possible, the library will assist users with the identification and mitigation of online risks.

## Staying Safe Online

To improve a user's chance of staying safe online there are certain precautions that can be taken, including:

- Keeping profiles set to private and checking settings regularly
- Think about personal safety before 'checking in' or using location based services
- Don't share personal information and be cautious of strangers online
- Managing digital reputation responsibly
- Respecting others and looking after each other online

## Cyber Bullying

Cyber bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, which is intended to harm others. The library does not condone any form of bullying via its electronic resources and facilities.

Cyber bullying can occur in the following forms:

- *Flaming* - sending angry, rude, vulgar messages directed at a person or persons privately or to an online group
- *Harassment* - repeatedly sending a person offensive messages
- *Denigration* - sending/posting rumours, harmful, untrue information about the person to others
- *Cyber stalking* - harassment that includes threats of harm or is highly intimidating
- *Impersonation or masquerading* - pretending to be another person and posting/sending material online to make them look bad
- *Outing or trickery* - tricking a person into sending information (secrets, embarrassing and personal information that can be used to send to others online
- *Exclusion* - excluding someone purposefully from an online group
- *Cyber stalking* – following someone through cyber space. Moving with them to different sites and applications; posting where they post



Cyber bullying can occur using the following applications:

- Email
- Social networking sites such as chat rooms, Facebook and Twitter
- Personal websites, blogs and forums
- Video and photo sharing sites such as YouTube, Vimeo, Instagram and Tumblr
- Mobile phone calls and SMS

Dealing with cyber bullying forms:

- Block the cyber bully and take a screenshot as evidence of the cyber bullying
- Report offensive material to the website administrator or service provider
- Talk to a friend or trusted adult
- Report it to **[www.esafety.gov.au](http://www.esafety.gov.au)**
- For more help, call the Kids Helpline (1800 55 1800) or contact the local police for non-urgent matters or 000 for emergencies

## Reporting Cyber Incidents

Depending on the nature of the issue, there are various methods to reporting cyber incidents. These methods are outlined on the Australian Government eSafety website ([www.esafety.gov.au](http://www.esafety.gov.au)) and include direct links to reporting incidents:

- **Website administrator** –to report issues about someone or something on their site
- **OCESC** – contact the Office of the eSafety Commissioner to report offensive, inappropriate or illegal material on a website ([www.esafety.gov.au](http://www.esafety.gov.au))
- **ScamWatch** –to report online scams and fraud ([www.scamwatch.gov.au/](http://www.scamwatch.gov.au/))
- **ACORN** – contact the Australian Cybercrime Online Reporting Network to report cyber crime and online incidents which may be breach Australian law ([www.acorn.gov.au](http://www.acorn.gov.au))
- **Police** – to report online child sexual exploitation

## Social Media

The library is not responsible or liable for, and does not endorse the privacy practices of social media websites and apps including Facebook, Instagram, Pinterest or Twitter. The library cannot control the practices and policies of social media websites. Your use of social media websites and apps is at your own risk.

## Disclaimer

Views expressed on social media website and apps via the library's facilities are not the views of this library, and the local government authority disclaims all liability for any such views, comments and advertising, or other non-LGA content.

The council does not endorse or control any advertising that may be displayed by social media websites and apps.

## **Complaints and Incidents**

This library takes incidents of misuse or abuse of technology very seriously. All members of the library community have a clear role to play in reporting such incidents. The library welcomes all complaints and feedback and encourages the community to work with the library in ensuring that incidents and accidents are not repeated.

## **Reporting Incidents and Accidents**

In the case of an incident or accident at this library, members of the public are asked to report to the nearest staff member who will take the appropriate action.

## **Legislative and Strategic Context**

This policy complies with the Western Australia Classification (Publications, Films and Computer Games) Enforcement Act 1996, Criminal Code Act 1995, Copyright Act 1968 and Albany Public Library's Public Internet Access Conditions of Use.