Council Policy – Public Use of Internet at Shire Libraries

Responsible Directorate	Community Development
Responsible Business Unit/s	Libraries
Responsible Officer	Manager Libraries
Affected Business Unit/s	Libraries ICT

Objective

The Shire of Ashburton (the Shire) is committed to providing a safe, welcoming environment and equitable access to materials and services for all library users.

The objective of this policy is to outline the obligations and responsibilities of all users of the internet at the Shire's public libraries.

This policy has been developed to provide smart, safe, and responsible use of technology within the libraries.

Scope

This policy applies to all library users.

Policy Statement

Acceptable use

Facilities and resources within the Shire's public libraries must be used in an acceptable and lawful manner by all users. Employees will work with the public to ensure compliance with this policy.

Principles of conduct

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

Ramifications

If an employee observes a patron using electronic facilities unlawfully or in violation of this policy the library user will be asked to immediately discontinue using the resource.

Continued misuse of library facilities will result in loss of privilege to use these resources and/or notification of activity to law enforcement officials.

User responsibilities

Overview

The Shire's public libraries are 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.

Furthermore, 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

Library users must:

- refrain from illegal or unethical use of the internet,
- perform their own computer activities, however employee assistance is offered subject to availability of resources,
- be responsible for their personal belongings, and it is at their own risk to leave any item unattended,
- provide and wear their own headphones to listen to any audio content,
- delete any of their own files or documents saved to a library computer or device,
- be responsible for any material they access during an internet session,
- be 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 of the library are reminded that all computers are in public areas which are 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 Shire has developed the following behaviour guidelines for all users of its in-house electronic resources:

- Users must be courteous and respectful to all other library users and employees,

- 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 employees where it is given,
- All equipment and resources are to be shared equally,
- Noise levels must be kept to a minimum and not cause disruptions to other library users,
- On request by a library employee, users may be required to end their computer session early or leave a computer area,
- Authorised room bookings will be given priority over individual user sessions,
- Where space permits, computers may be used by two or more people providing their behaviour is not disruptive,
- Users may not invade the privacy of others, or attempt to modify or gain access to files, passwords or data belonging to others,
- 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 this policy and State and Commonwealth legislation.

Supervision of minors

Employees of the Shire's libraries are not responsible for supervising minors. Supervision or restriction of a minor's access to the internet is the responsibility of the parent or guardian. Some material available on the internet is unsuitable for minors. Parents or guardians are encouraged to educate and work with their children when using technology.

Ramifications

If a user does not present acceptable responsibility or behaviour, he or she may be banned from using library facilities or asked to leave the premises. Library employees reserve the right to contact law enforcement officials if the matter is not resolved.

Filtering

The Shire reserve the right to filter material deemed inappropriate or illegal in accordance with Part 7 of the *Western Australia Classification (Publications, Films and Computer Games) Enforcement Act 1996*.

Although most online content is made available, the Shire strives to minimise the possibility of illegal/inappropriate material being accessed in a public environment.

Fixed computer access

The library's fixed computer access terminals use web security services to filter certain online content. 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.

Web privacy

Overview

The Shire's public libraries adhere to the *Privacy Act 1988*.

The following web privacy provisions outline how the library deals with personal information related to our electronic resources.

Browsing privacy

Where possible, the library will configure the internet browser's privacy options on fixed computer access terminals to prevent browsing history, temporary internet files, form data, cookies, and usernames and passwords from being retained by the browser. Each computer will be reset at the end of each session and any retained data will be deleted.

It is the responsibility of the user to end their session before leaving to ensure this process is initiated. All websites a user attempts to access on a fixed computer access terminal will be logged through the Shire's firewall service. Information held in the log includes the date, time, computer number, and the URL of each website a user has attempted to access.

The logs do not hold any user identifying information. Information collected is only accessible by Shire ICT employees, if required.

The library's wireless internet service will retain information on filtered content.

The log includes the date and time of attempted access, the device MAC address and name, and the filtering rule triggered.

Monitoring

The Shire reserves the right to monitor and inspect without consent, any data on a computer system connected to the Shire's network.

Such inspections will occur to prevent, detect, and minimise the unacceptable usage of the computer system.

Collection of personal information

A user's device MAC address and device name will be recorded when a user accesses the library's wireless internet service.

These records are only accessible by the wireless internet provider.

Online databases subscribed to by the library may record a registered user's account information including library card number, email address, given name, and surname.

Databases that provide a lending service (such as for eBooks, eAudiobooks and eMagazines), will also record the title and date borrowed of items loaned. Browsing activity through these databases is recorded anonymously.

Cyber safety

Overview

The Shire has a responsibility to provide a safe environment to the 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, and
- 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 Shire 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 – is repeatedly sending a person offensive messages.
- Denigration – sending/posting rumours, harmful, untrue information about the person to others.
- Cyber stalking – following someone through cyberspace. Moving with them to different sites and applications; posting where they post.
- 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 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

- Block the cyber bully
- 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
- For more help, call the Kids Helpline (1800 55 1800) or contact the police (131 444 for non-urgent matters or 000 for emergencies).

Reporting cyber incidents

There are various methods to reporting cyber incidents.

These methods are outlined on the Australian Government eSafety website and include direct links to reporting incidents:

- Website administrator – contact the website to report issues about someone or something on their site.
- ACMA – contact the Australian Communications and Media Authority to report offensive, inappropriate or illegal material on a website.
- ScamWatch – contact ScamWatch to report online scams and fraud.
- Police – report online child sexual exploitation.

Social media

Overview

The Shire 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 library facilities are not the views of the Shire, and the Shire disclaims all liability for any such views, comments, advertising, or other non-Shire content.

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

The Shire reserves the right to remove comments posted to its social media accounts at its sole discretion in accordance with this policy.

Complaints and incidents

The Shire 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 libraries welcome all complaints and feedback and encourages the community to work with the libraries in ensuring that incidents and accidents are not repeated.

Definitions

Cyber safety means the safe use of Information and Communication Technologies (ICT) equipment or devices (including cellular phones) and the internet.

Cyber bullying means the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

eResources means electronic resources such as databases and exclusive online content.

Fixed computer access means individual stationary computer terminals that offer internet access and an office suite of desktop programs.

Wireless internet means wireless connectivity to the internet on a person's home computer, laptop, smartphone, or similar mobile device.

Minor means a person under the age of 18 years.

Relevant policies/documents

Nil

Relevant legislation/local laws

Western Australia Classification (Publications, Films and Computer Games) Enforcement Act 1996
Criminal Code
Copyright Act 1968

Office use only				
Relevant delegations	Nil			
Council adoption	**Date**	14 February 2023	**Resolution #**	019/2023
Reviewed/modified	**Date**		**Resolution #**	
	Date		**Resolution #**	
	Date		**Resolution #**	
Next review due	2027			