Southern Grampians

SHIRE COUNCIL

Public IT Use POLICY

Policy Name	Public IT Use
File Location	D/17/45771
Document status	Final
Version	1.0 – Policy documents are amended from time to time, therefore you should not rely on a printed copy being the current version.
Version Date	06/02/18
Next Review date	01/02/22

TABLE OF CONTENTS

1. Aim

Southern Grampians Shire Council (Council) is committed to providing a safe, welcoming environment and equitable access to materials and services for all.

The aim of this Policy is to outline the obligations and responsibilities of all users of Councils public IT resources and internet. This Policy has been developed in order to provide smart, safe and responsible use of Council provided technology located within the Shire.

2. Application

This Policy applies to all users of Council provided IT resources and internet.

3. Responsibilities

It is the responsibility for all public users of Council provided IT resources and internet to read and comply with the Policy.

4. Scope

This Policy applies to all users of Council's public IT resources and internet. The resources include but are not limited to, computer and internet access, scanning and printing services, kiosk machines and use of online databases.

5. 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
IT resources	Examples of IT resources are shown below, note this is not a finite list: • Library Public Computer • Digital display terminal • Kiosk touchscreen terminal • SGSC provided Public Internet
Library	Greater Hamilton Library and Mobile Library
MAC Address	A media access control address (MAC address) of a device is a unique identifier assigned to network device
Minors	A person under the age of eighteen (18) years
Unethical use	Examples of unethical use are shown below, note this is not

	a finite list: • Pirating • Hacking • Invasion of privacy • Bullying • Exploitation • Identity theft
URL	Uniform Resource Locator (URL) is used to specify addresses on the World Wide Web
Web filter	A Web filter is a program that can screen the contents of an incoming Web page to determine whether some or all of it should not be displayed to the user.
Wireless Internet	Wireless connectivity to the Internet on a person's home computer, laptop, smartphone or similar mobile device.

6. Acceptable Use

Council's publicly accessible IT resources and Internet must be used in an acceptable and lawful manner by all users. Staff will work with the public to ensure compliance with this Policy for responsible use at all times.

6.1 Principles of Conduct

This policy aims to promote rewarding, responsible and equitable use of the public IT resources and internet provided by Council.

6.2 Compliance with Legislation

This Policy should be read in conjunction with all other relevant Council policies and procedures, as well as relevant legislative requirements. The list below is not complete and is a guide only because legislation continually changes and new legislation is continually being applied.

Related Legislation:

- Classification (Publications, Films and Computer Games) Enforcement Act 1995
- Criminal Code Act 1995
- Copyright Act 1968

The complete and up-to-date collection of Commonwealth legislation can be viewed on the Australian Government ComLaw website, www.comlaw.gov.au. Victorian Legislation can be viewed on the Victorian Legislation and Parliamentary Documents website, http://www.legislation.vic.gov.au/.

6.3 Inappropriate use and breach of policy

If a member of staff observes a user unlawfully using electronic facilities, in breach of Council policies or committing an offence as outlined in section '*Compliance with Legislation*', the user/s will be asked to immediately discontinue using the resource. A member of staff will be required to complete an Incident Report as outlined in section '*Complaints and Incidents*'. Misuse of Council IT resources may result in loss of privilege to use these resources and/or notification of activity to law enforcement officials.

7. User Responsibilities

Council is committed to providing an environment that is free from harassment, discrimination and bullying. All users of Council public IT resources and Internet are expected to behave in an appropriate manner and respect all other people and facilities. IT resources and facilities are expected to be used for the purpose 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 of these resources.

7.1 Responsibilities

- Refrain from illegal or unethical use of the Internet
- Users must perform their own computer activities, however when using the public PCs in the Library, staff assistance is offered subject to availability
- Users of the Library must provide and wear their own headphones to listen to any audio content
- Users are responsible for deleting any of their own files or documents saved to a Council 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.

7.2 Behaviour

Users of the public Council IT resources and Internet are reminded that access is provided 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, Council has developed the following behaviour guidelines for all users of public IT resources and Internet:

- Users must be courteous and respectful to all other users
- Internet access provided by Council 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
- 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 all related Council policies and State and Commonwealth legislation.

7.3 Supervision of Minors

Council is 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.

8. Filtering

Council reserves the right to filter material deemed inappropriate or illegal. Although the majority of online content is made available, Council strives to minimise the possibility of illegal/inappropriate material being accessed in a public environment.

8.1 SGSC Public Web Filters

Council implement web security services to filter certain online content that can be accessed via Council's public internet service. Council has the right to block content that may harm its property and/or network, or content that may distress or upset other users.

The following categories are filtered:

- **Adult Material** – Sites that contain adult-oriented categories may also contain age-restricted content. This category includes the following:
    - Nudity – Sites that offer depictions of nude or semi-nude human forms, singly or in groups, not overtly sexual in intent or effect
    - Adult Content – Sites that display full or partial nudity in sexual context, sexual activity, erotica, sexual paraphernalia, sex-oriented businesses including clubs, nightclubs, escort services and sites supporting the online purchase of such goods and services
    - Sex – Sites that depict or graphically describe a sexual act or activity, including exhibitionism and sites offering direct links to such sites
    - Lingerie and Swimsuit – Sites that offer images or models in suggestive but not lewd costume, with semi nudity permitted. Includes calendar and pinup art and photography. Includes sites offering lingerie or swimwear for sale
- **Bandwidth** - This category includes the following:
    - Peer-to-Peer file sharing – Sites that provide client software to enable peer-to-peer file sharing and transfer
    - Surveillance – Sites that enable real-time monitoring of various operations via network cameras, webcams and other video recording devices
- **Extended Protection** – This category includes the following:
    - Emerging Exploits – Sites found to be hosting known and potential exploit code
- **Illegal or Questionable** - Sites that provide instruction in or promote, non-violent crime or unethical or dishonest behaviour or the avoidance of prosecution.

- **Information Technology** - Sites sponsored by, or providing information about, computers, software, the Internet and related business firms, including sites supporting the sale of hardware, software, peripherals and services. This category includes the following:
    - Proxy avoidance – Sites that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server.
    - Unauthorised Mobile Marketplaces – Protects against websites that may distribute applications unauthorised by the mobile OS manufacturer, the handheld device manufacturer or the network provider. Traffic visiting websites in this category may indicate jail-broken or rooted phones.
- **Intolerance** – Sites that condone intolerance towards any individual or group.
- **Militancy and Extremist** – Sites that offer information about, or promote or are sponsored by, groups advocating anti-government beliefs or action.
- **Productivity** – The parent category that contains the following categories:
    - Online Brokerage and Trading – Sites that support active trading of securities and investment management
    - Pay-to-Surf – Sites that reward users for online activity such as viewing websites, advertisement or email
- **Security** – Security-related website categories that allow users to develop polices to block access to sites associated with spyware, phishing, key logging and malicious mobile code.
    - Malicious Web Sites – Sites containing code that may intentionally modify users systems without their consent and cause harm
    - Spyware – Sites that download software that generate HTTP traffic (other than simple user identification and validation) without a user's knowledge.
    - Phishing and Other Frauds - Sites that counterfeit legitimate sites to elicit financial or other private information from users
    - Key loggers - Sites that download programs that record all keystrokes, and which may send those keystrokes (potentially including passwords or confidential information) to an external party
    - Bot Networks - Sites that host the command-and-control centres for networks of bots that have been installed onto users' computers (Excludes web crawlers)
    - Malicious Embedded Link - Sites infected with a malicious link
    - Malicious Embedded Iframe - Sites infected with a malicious iframe
    - Suspicious Embedded Link - Sites suspected of being infected with a malicious link
    - Mobile Malware - Protects against malicious websites and applications designed to run on mobile devices
    - Advanced Malware Command and Control - Protects against outbound transmissions from a compromised machine to a malicious command-and-control centre
    - Compromised Websites - Sites that are vulnerable and known to host an injected malicious code or unwanted content.

- **Tasteless** – Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to improper language, humour or behaviour.
- **Violence** – Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.

9. Bandwidth Throttling and Capping

The public internet service offered by Council over Wi-Fi is throttled and capped to regulate network traffic and minimise bandwidth congestion.

A throttling setting of 5MB/s and a daily download cap of 300MB per device per day is in place across all Council Wi-Fi public internet services. Additional Wi-Fi download capacity will be made available for purchase via the Council public Wi-Fi portal.

No throttling or capping is applied to the Council public internet provided via the fixed public PC's offered in the Library.

10. Web Privacy

Council adheres to the Privacy Act 1988, Schedule 3 - National Privacy Principles and the Privacy and Data Protection Act 2004. The following Web Privacy clauses outline how the Library deals with personal information related to our electronic resources.

10.1 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 user names and passwords from being retained by the browser. Each computer will be reset at the end of each working day and any retained data will be deleted.

All websites that a user attempts to access using Council's public internet service will be logged through the Council firewall service. Information held in the log includes the date, time, MAC address, device name and the URL of each website a user has attempted to access. The logs do not hold any user identifying information.

10.2 Monitoring

Council reserves the right to monitor and inspect without consent, any data on a Council-provided device connected to the Council network. Such inspections will occur to prevent, detect and minimise the unacceptable usage of the computer system.

10.3 Collection of Personal Information

A user's device MAC address and device name will be logged when a user accesses the Council public Wi-FI internet service. The logs do not hold any user identifying information.

11. Cyber Safety

Council 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.

11.1 Staying Safe Online

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

- Keeping social media profiles set to private and checking settings regularly
- Thinking about personal safety before 'checking in' or using location based services
- Sharing personal information and being cautious of strangers online
- Managing digital reputation responsibly
- Respecting others and looking after each other online.

11.2 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. Council 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
- 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 or personal information) that can be used to send to others online
- Exclusion - excluding someone purposefully from an online group
- Cyber-stalking – harassment that includes threats of harm or is highly intimidating. Following someone through cyberspace. Moving with them to different sites and applications; posting where they post.

Cyber bullying can occur using applications including but not limited to:

- 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 (5551 9100 for non-urgent matters or 000 for emergencies)

11.3 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 Cybercrime Online Reporting Network (ACORN) www.acorn.gov.au and include direct links to reporting incidents.

If you believe you or someone else is in physical danger, contact the necessary law enforcement officials.

12. Social Media

Council is not responsible or liable for, and does not endorse the privacy practices of social media websites and applications such as Facebook, Instagram, Pinterest or Twitter. Council cannot control the practices and policies of social media websites. Your use of social media websites and applications is at your own risk.

12.1 Disclaimer

Views expressed on social media websites and applicaitons via Council facilities are not the views of Council, and Council disclaims all liability for any such views, comments, advertising or other non-Council content.

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

Council reserves the right to remove comments posted to its social media accounts at its sole discretion based on the Acceptable Use policy and Social Media policy.

13. Complaints and Incidents

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

13.1 Lodging Complaints

Complaints can be made by contacting Customer Services on (03) 5573 0444 or emailing Council at council@sthgrampians.vic.gov.au.

13.2 Reporting Incidents and Accidents at the Library

In the case of an incident or accident at Council Library, members of the public are asked to report to the nearest staff member who will take the appropriate action. Council Library staff members are required to fill out an Incident Form as a record of any incidents or accidents which are reported or witnessed.

14. Review

This Policy will be reviewed every four (4) years or in line with legislative changes.

APPROVED	Chief Executive Officer	Michael Tudball	
DATED	8/3/18		