AP004 – Information Communication Technology

1. Intention

To ensure the conditions of usage of all Information & Communication Technology (ICT) facilities provided by the Shire of Waroona.

This policy outlines appropriate use of the Shire of Waroona's electronic communications and systems and applies to all elected members, employees, Shire volunteers and other users of the Shire's information, communication, and technology systems.

2. Scope

This policy applies to:

- Elected Members;
- All workers whether by way of appointment, secondment, contract, temporary arrangement or volunteering, work experience, trainees, and interns;
- Any external party involved in providing goods or services to the Council, such as contractors, consultants, outsourced service providers and suppliers;
- All users of Shire of Waroona ICT systems regardless of work location; and
- The use of all aspects of Shire of Waroona ICT systems, networks, software, and hardware collectively referred to as **"Shire of Waroona ICT systems".**

3. Definitions

Authorised persons means the Chief Executive Officer (CEO) or a person authorised by the CEO of the Shire of Waroona.

Cth denotes the Commonwealth of Australia.

Electronic communications means email, instant messaging and any other material sent electronically.

Malicious Software commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Multi-factor Authentication (MFA/2FA) is defined as 'a method of authentication that uses two or more authentication factors to authenticate a single user to a single user authentication verifier. The authentication factors that make up a multi-factor authentication request must come from two or more security principles, such as a person, device, service or application.

Paraphase is similar to a password, however, instead of making up an actual word using letters, numbers and symbols, a sentence is used instead.

Personal use means all non-work related use, and includes internet usage and private emails.

Shire of Waroona ICT Systems includes but is not limited to, Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), CCTV systems, Radio systems, Intranet, Extranet, Internet, electronic mail (email), computer systems, software, servers, desktop computers, notebook computers, mobile phones, digital cameras, hand held devices (for example, personal digital assistants or "PDAs"), USB memory sticks and other ICT portable storage devices.

Users of Shire of Waroona ICT systems includes all elected members, all employees (including ongoing, casual, temporary employees and volunteers) and contractors engaged in Shire of Waroona and external users who connect to the Shire of Waroona ICT system for the purposes of electronic business.

4. Statement

The Shire provides Information & Communication Technology systems for the purposes of improving and enhancing the conduct of business and functions of the Shire, and the provision of such should be managed to ensure that it is used in an appropriate manner.

The Shire seeks to manage usage of the Shire of Waroona ICT systems through the development and implementation of this policy. The policy must be adhered to, with legal and ethical considerations and consistent with the aims, values and objectives of the Shire of Waroona, whenever using the Shire's ICT systems.

4.1 Area of Application

This policy governs the use of the Shire of Waroona's ICT systems and includes but is not limited to:

(a) Publishing and browsing on the internet (including Intranet and Extranet);
(b) Downloading or accessing files from the Internet or other electronic sources;
(c) Email;
(d) Electronic bulletins/notice boards;
(e) Electronic discussions/news groups;
(f) Weblogs ('blogs');
(g) File transfer;
(h) File storage;
(i) File sharing;
(j) Video conferencing;
(k) Streaming media;
(l) Instant messaging/mobile phone text messaging;
(m) Online discussion groups and 'chat' facilities;
(n) Subscriptions to list servers, mailing lists or other like services;
(o) Copying, saving or distributing files;
(p) Viewing material electronically;
(q) Printing material; and
(r) Social media.

4.2 Applicable Legislation/Policy

Any reference in this policy to an Act, Regulation, Guidelines, Code of Conduct or other document includes a reference to the Act, Regulation, Guidelines, Code of Conduct or other document as amended from time to time. Users of the Shire of Waroona ICT system are also subject to Acts and Regulations not explicitly referenced in this policy. These include, but are not limited to:

(a) *Privacy Act 1988* (Cth)
(b) *Freedom of Information Act 1982* (Cth)
(c) Freedom of Information Act 1992
(d) *Crime Act 1914* (Cth)
(e) *Criminal Code Act 1995* (Cth)
(f) *Australian Crimes Commission Act 2002* (Cth)
(g) State Records Act 2000
(h) *Spam Act 2003* (Cth)

The Shire of Waroona Code of Conduct applies in the application of this policy.

4.3 Responsibility

It is the responsibility of the CEO, the Directors and Managers to ensure that employees and elected members to whom this policy applies are aware of this policy. This may include, but is not limited to:

(a) Providing access to a copy of this policy;
(b) Reminders of the need for compliance with the policy; and
(c) Providing updates or developments of the policy to those affected by the policy.

It is the responsibility of all users to abide by the policy.

5. Policy Measures

5.1 Business Purposes

The Shire of Waroona's ICT systems are tools to be used for business purposes and must:

(a) Be for Shire business purposes only, or where authorised or required by law, or with the express permission of an authorised person; and
(b) Be used like other business communications and comply with any Codes of Conduct or legislative requirements that apply to the user.

Notwithstanding clause 5.1(a), users of the Shire of Waroona ICT systems may use the Shire of Waroona's ICT systems for personal use provided the use is minor and infrequent and does not breach this policy. Users must not engage in excessive personal use of the Shire of Waroona's ICT systems during working hours. Users must not engage in excessive personal use of electronic communications and the internet using Shire of Waroona networks outside of office hours. A breach of either of these constitutes a failure to abide by this policy.

Subject to minor and infrequent personal use in accordance with this clause:

(a) Subscribing to list servers (LISTSERVS), mailing lists and other like services must be for Shire of Waroona purposes or professional development reasons only; and
(b) Online conferences, discussion groups or other like services must be relevant and used for Shire of Waroona purposes or professional development activities. Such interaction requires that internet etiquette should be observed along with current societal standards for respect and fairness.

Obtaining unauthorised access to electronic files of others or to email or other electronic communications of others, is not permitted and may constitute a criminal offence.

Large downloads or transmissions should be minimised to ensure the performance of the Shire's ICT systems for other users is not adversely affected. Where a user has caused the Shire to incur costs for excessive downloading of non-work related material in breach of this policy, the Shire may seek reimbursement or compensation from the user for all or part of these costs or apply other forms of disciplinary action.

5.2 Shire Property

Shire of Waroona is the owner of and asserts copyright over:

(a) All electronic communications created by employees as part of their employment and use of the Shire's ICT systems.
(b) All electronic data/information stored on the Shire's ICT systems.

(c) Personal devices if they are fitted with the Shire's ICT software.

Electronic communications created, sent or received by the users referred to in item 4.1 of this policy are the property of the Shire, and may be accessed as records of evidence in the case of an investigation. All electronic communications are kept as per the Shire's Record Keeping Plan and legislation. Electronic communications may also be subject to discovery in litigation, freedom of information applications and criminal investigations. Email messages and mobile phone text messages may be retrieved from back-up systems. This clause is subject to Commonwealth or State law that precludes such access.

5.3 Monitoring

Use of the Shire's ICT systems may be monitored by authorised persons. Shire employees shall have no expectation of privacy in anything they store, send or receive on the Shire's ICT systems. The Shire may monitor messages without prior notice. The Shire is not obliged to monitor email messages.

Authorised persons may examine or monitor the records of the Shire's ICT systems including for operational, maintenance, compliance, auditing, security or investigative purposes. For example, electronic communications and web sites visited may be monitored. The Shire may investigate a complaint arising from the use of the Shire's ICT systems. Use of the Shire's ICT systems constitutes consent to monitoring in accordance with this policy.

If at any time there is a reasonable belief that the Shire's ICT systems are being used in breach of this policy, the CEO or the Director or Manager of the person who is suspected of using the Shire's ICT systems inappropriately may suspend all or any part of that person's use of the Shire's ICT systems and remove access to the equipment while the suspected breach is investigated.

5.4 Defamation

Electronic communications may be easily copied, forwarded, saved, intercepted, or archived. The audience of an electronic message may be unexpected and widespread. The Shire's ICT systems must not be used to send information or material that defames an individual, organisation, association, company or business.

5.5 Copyright Infringement

Copyright material (software, database files, documentation, cartoons, articles, graphic files, music files, video files, photos, text and downloads) from third parties must not be used without specific authorisation to do so.

The Shire supports the rights of copyright owners and does not tolerate deliberate copyright use. Copyright material will be deleted if discovered.

5.6 Illegal Material

The Shire's ICT systems must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the WA Police or other relevant authority and will be viewed as a serious breach of the terms of employment and appropriate action taken.

Illegal or unlawful use includes the use of:

- Defamatory material;
- Pornography;
- Material that could constitute racial or religious vilification;
- Unlawfully discriminatory material;

- Bullying;
- Stalking;
- Use which breaches copyright law;
- Fraudulent activity; and
- Computer crimes and other computer offences under various Crimes Acts.

5.7 Offensive or Inappropriate Material

Use of the Shire's ICT systems must be appropriate to a workplace environment. This includes but is not limited to the content of all internal and external electronic communications.

The Shire's ICT systems must not be used for material that is:

- Threatening;
- Offensive;
- Discriminatory;
- Obscene;
- Abusive;
- Sexist;
- Racist;
- Hateful;
- Harassing; or
- Pornographic.

This includes sexually orientated messages or images that could constitute sexual harassment. All Shire elected members and employees should be familiar with any of the Shire's anti-discrimination, equal opportunity, and harassment policies.

Users of the Shire's ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their reporting officer immediately. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of such material be asked to refrain from sending such material again. Such material should not be forwarded internally or externally or saved onto the Shire's ICT system except for the purposes of investigating a breach of this policy.

5.8 Malicious Software

Electronic communications are potential delivery systems for various forms of computer viruses. All data, programs and files which are downloaded electronically or attached to messages or imported on any other media (portable storage devices) should be scanned by an anti-virus program before being launched, opened or accessed. Do not open any downloaded files, emails or attachments that you are not expecting or that look suspicious. Any suspicious emails or attachments should be reported to the ICT contractor immediately.

5.9 Attribution

False attribution of breaches of this policy may occur. Communications can be modified, or intercepted to reflect a false message, sender, or recipient. If a user suspects that they are communicating with an imposter or receiving fraudulent information, they should report the matter to the ICT contractor immediately.

5.10 ICT Assets

To mitigate the potential security risks of using outdated technology and to ensure increased efficiencies and productivity, the Shire will maintain a four-year cycle of the replacement of ICT assets including:

(a) Desktop PC's;
(b) Notebooks/Laptops;
(c) Servers; and
(d) Photocopiers.

ICT software will be upgraded as required and on advice from ICT contractors.

5.11 ICT Equipment Inventory

The Shire should maintain full control of the supervision and physical location of all Shire ICT equipment. All Shire ICT equipment and allocation should be recorded in the Shire's Minor Assets Inventory system. Shire ICT equipment should not be provided to another party without notification to the ICT contractor or Corporate Services representative.

5.12 Security and Passwords

User ID's and passwords should be kept secure and confidential. User ID's and passwords should not disclosed to anyone, including disclosures to Reporting Officers or above. Users must not facilitate unauthorised access to the Shire's ICT systems through the disclosure or sharing of passwords or other information designed for security purposes. Passwords must:

(a) Be a minimum length of 10 characters and a maximum length of 15 characters;
(b) Have some complexity containing a combination of letters both lower and uppercase, numbers and symbols;
(c) Not include your name, title or commonly guessed names (partner or child's name etc);
(d) Expire at regular intervals;
(e) Be changed when requested by the system or when it is suspected that it may have been compromised;
(f) Be treated as sensitive and confidential and must not be shared;
(g) Not be recorded in the 'remember password' feature of any application for any Shire passwords/passphrases under any circumstances; and
(h) Use MFA or 2FA where it is available to be used for an application or online service.

5.13 Remote Access

Remote access is provided to network users who are in possession of a portable device (notebook) using remote access technology. As a de facto extension of the Shire's network, users with remote access are subject to the same rules and conditions that apply to the Shire's owned equipment.

The following conditions apply to elected members and employees with remote access:

(a) All the requirements of this policy apply to the use of remote access.
(b) Family members must not be provided with access to the Shire's ICT and must not violate any of the Shire's policies, perform illegal activities, or use the access for outside business interests. Responsibility rests with the approved user for any consequences that arise from misuse.
(c) The device that is connected remotely to the Shire's network is not to be connected to any othe network at the same time, with the exception of personal networks that are under complete control of the user.

(d) The use of non-shire email accounts (ie. Hotmail, yahoo) should not be used for the purposes of conducting Shire business.
(e) Non-standard hardware configurations and security configurations for access to hardware must be approved by the ICT contractor.

5.14 Back-ups, Disaster Recovery & Incident Response

The Shire will ensure that procedures are in place with the ICT contractor for the regular back-up and secure storage of critical data and information. The Shire's ICT Recovery Plan has been designed to ensure the continuation of vital business processes in the event that an incident, disruption, crisis, disaster or emergency occurs. The plan aims to provide an effective solution that can be used to recover key business processes within the required timeframe using backup data stored either onsite or offsite.

5.15 Mass Distribution and Spam

The use of electronic communications for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited. Mass electronic communications should only be sent in accordance with normal Shire procedures.

The use of electronic communications for sending unsolicited commercial electronic messages ('spam') is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

5.16 Records Management

Electronic communications are public records and subject to the provisions of the State Records Act 2000.

The Shire's record management practices for management of email messages must comply with the Shire of Waroona Record Keeping Plan.

5.17 Non-compliance

Inappropriate use of the Shire's ICT systems and non-compliance with this policy may constitute:

(a) A breach of employment obligations;
(b) Serious misconduct;
(c) Sexual harassment;
(d) A criminal offence;
(e) A threat to the security of the Shire's ICT systems;
(f) An infringement of the privacy of staff and other persons; or
(g) Exposure to legal liability.

Non-compliance with this policy will be regarded as a serious matter and appropriate action may be taken.

Where there is reasonable belief that an illegal activity has taken place, the matter may be referred to WA Police.

5.18 Termination

Access is to be terminated for elected members and employees to the Shire's ICT systems when access is no longer required and included as part of the Shire's termination checklist. Any shire owned devices will be cleared by ICT, and communications redirected.

6. Legislative and Strategic Context

Privacy Act 1988 (Cth)
Freedom of Information Act 1982 (Cth)
Freedom of Information Act 1992
Crime Act 1914 (Cth)
Criminal Code Act 1995 (Cth)
Australian Crimes Commission Act 2002 (Cth)
State Records Act 2000
Spam Act 2003 (Cth)

7. Review

This policy is to be reviewed triennially.

8. Associated Documents

Nil.

Division	Administration				
Policy Number	AP004				
Contact Officer	Director Corporate Services				
Related Legislation	Nil				
Related Shire Documents	AMP003 – Information Communication Technology				
Risk Rating	Medium	**Review Frequency**	Triennially	**Next Review**	July 2027
Date Adopted	18/12/2018				OCM18/12/126

Amendments		
Date	**Details of Amendment**	**Reference**
22/06/2021	Updated as part of major review and reformatted.	OCM21/06/071
23/07/2024	Policy re-written. New content added	OCM24/07/108
Previous Policies		
CORP053 – Information Communication Technology		