Information Management and Information and Communications Technology (ICT) Acceptable Use Policy

Introduction

The Shire relies on secure and responsible Information Management (IM) and Information and Communications Technology (ICT) systems to support service delivery, ensure business continuity, and protect corporate information. This policy outlines the acceptable use of the Shire's ICT resources and information systems to ensure compliance with legislative obligations and to meet audit expectations.

Objective

This policy aims to:

(a) Uphold the legislative and administrative requirements for the use of IM and ICT resources within the Shire.

(b) Ensure all authorised users understand their obligations regarding the use, protection, and accessing of Shire information systems.

(c) Maintain confidentiality, integrity, availability, compliance, and responsibility in managing information assets.

(d) Support the Shire's commitment to the *State Records Act 2000* and other relevant legislation.

(e) Establish a consistent, auditable framework that satisfies the 2024/2025 audit requirements.

Scope

This policy applies to all employees, contractors, elected members, volunteers, and any other authorised users who access or use the Shire's:

(a) ICT equipment (including desktops, laptops, mobile devices, networks and peripherals);

(b) Software, applications, and cloud services;

(c) Information systems and data repositories; and

(d) Electronic communications tools (e.g., Microsoft Outlook, mobile email, instant messaging).

Definitions

Term	Definition
Authorised Persons	A member of the Executive or ICT contractor including delegated representatives.

Term	Definition
Authorised User	Any person granted authorised access to systems and services
BYOD	Bring Your Own Device.
Corporate Knowledge	Any file, record, communication thread, or intellectual property that holds business value
Electronic Communications	Email, instant messaging, and any material sent electronically.
Information System	Any organised system for collecting, storing, and communicating information.
Malware	Software designed to cause damage or unwanted action
Record	Any "recorded information", including documents, maps, diagrams, graphs, images, audio, or electronically stored information
Records and Document Management	Any system or service responsible for corporate data storage or filing
Misconduct	Unacceptable or improper behaviour as defined in the Shire's Code of Conduct.
Refer to the Corporate Documents Glossary	https://www.toodyay.wa.gov.au/documents/470/corporate-documents-glossary-(definitions)

Policy Statement

All authorised users must comply with this Policy to mitigate operational, security, legal and reputational risks to the Shire. Ensuring secure and appropriate use of ICT systems is essential to business continuity, the protection of corporate information, and compliance with legislation.

1. Information Security Principles

The Shire applies five information security principles:

(i) **Confidentiality** – Only authorised users may access information.

(ii) **Integrity** – Information must remain accurate and complete.

(iii) **Availability** – Information must be accessible when required.

(iv) **Compliance** – All use must comply with legislation and Shire policy.

(v) **Responsibility** – Authorised Users must not negatively affect other systems or other authorised users.

The Shire's ICT systems and information security practices will align with the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model and other applicable cybersecurity standards.

2. Information and ICT Asset Classification

Information and ICT assets must be classified according to sensitivity and risk:

(a) Public – Information approved for public release

(b) Internal – Operational information not intended for public distribution

(c) Confidential – Sensitive business or personal information requiring restricted access

(d) Highly Sensitive – Critical systems, executive information, or data requiring the highest level of protection

Handling requirements must align with classification, including:

(a) access control;

(b) storage requirements;

(c) transmission protection; and

(d) disposal procedures.

3. Records and Information Management

(a) All records must be registered in the corporate Records Management System and must be complete and accurate.

(b) Ownership of all corporate records rests with the Shire.

(c) Records must be retained or disposed of in accordance with State Records Commission schedules.

(d) Records of historical or cultural significance must be preserved.

4. Acceptable Use of Information and Communications Technology (ICT) Systems

Authorised users must not bypass security controls; install unauthorised software or applications; or use unauthorised cloud storage services.

The following activities are also prohibited:

(a) Interfering with intended use of resources (e.g., excessive downloads or bandwidth use).

(b) Attempting to gain unauthorised access.

(c) Using systems to defraud, misrepresent, or obtain information unlawfully.

(d) Breaching privacy.

(e) Conducting private business or commercial activity.

(f) Publishing offensive or discriminatory content.

(g) Misrepresentation of the Shire.

5. User Accounts and Passwords

(a) All authorised users must have unique network IDs and secure passwords.

(b) Passwords must not be shared, revealed, or stored in conspicuous locations.

(c) Accounts lock after three failed login attempts.

(d) Authorised users must report suspected compromises immediately.

6. Internet and Email Use

Limited personal use of ICT systems is permitted, provided that such use:

(a) does not interfere with work duties;

(b) does not incur additional cost to the Shire;

(c) complies with this policy and all relevant legislation; and

(d) does not expose the Shire to security, legal or reputational risk.

6.1 Internet Use

(i) Must not be used in ways that cause offence, reputational damage or performance issues.

(ii) Authorised users must avoid downloading harmful content or compromising security.

(iii) Access to inappropriate websites may be automatically blocked.

6.2 Email Use

(i) Email is for official Shire business only;

(ii) Emails are business records and must be filed into the Records Management System;

(iii) Elected Members must ensure that all their communications relating to Shire business are captured in accordance with the *State Records Act 2000*.

(iv) Where required, communications must be forwarded to the designated Shire recordkeeping system to ensure compliance with legislative recordkeeping obligations. Guidance will be provided to Elected Members regarding what information must be retained and how privacy is protected.

(v) Spam, chain letters, and offensive messages are prohibited.

7. Software, Mobile Devices & Physical Security

(a) Only the ICT Contractor may install software;

(b) All software must be licensed and used according to license terms;

(c) Authorised Users must safeguard mobile devices. as much as practicable.;

(d) Physical and environmental risks to information and equipment must be mitigated.

8. Remote Access, BYOD and Cloud Services

(a) Remote access, BYOD, and cloud services must comply with Shire ICT security standards.

(b) The CEO is responsible for ensuring that secure access systems and controls are in place.

(c) Technical approvals, configuration and access management are administered by authorised ICT personnel in accordance with approved standards.

9. System Monitoring and Audit Logging

The Shire will implement monitoring and logging of ICT systems to:

(a) detect and respond to security incidents;

(b) protect information assets; and

(c) support audit and compliance requirements.

Monitoring must:

(a) be conducted in accordance with relevant privacy and legislation;

(b) ensure access to logs is restricted to authorised personnel; and

(c) retain records in accordance with the State Records Act 2000.

10. Incident Response

All suspicious or irregular ICT events must be reported immediately in accordance with the Shire's Data Breach and Incident Management procedures.

All suspicious or irregular ICT events must be:

(a) Reported;

(b) Investigated;

(c) Addressed promptly;

(d) Evaluated for business impact; and

(e) Routine helpdesk requests must be emailed to support@xl2.au.

11. Roles and Responsibilities

(a) CEO

- Provides and implements ICT assets, systems and processes.
- Ensures monitoring systems are in place and effective.
- Ensure ICT governance, cybersecurity frameworks and controls align with approved standards and legislative requirements.

(b) Executive and Supervisors

- Promote good information management practices.
- Ensure training and adherence to records and ICT directives.

(c) Employees, Elected Members & All Authorised Users

- Adhere to all ICT and records management directives.
- Create and maintain accurate records as part of corporate responsibility.

12. Breaches and Consequences

Breaches may result in:

(a) Security incidents including malware, data loss or privacy breaches;

(b) Legal consequences;

(c) Disciplinary action under the Code of Conduct; and

(d) Notification to law enforcement or the Crime and Corruption Commission.

Flow Charts (if necessary)

The Office of the Auditor General (OAG) published report 9: 2023-24 6 December 2023 for Implementation of the Essential Eight Cyber Security Controls which include:

Reference Information

- Privacy Management Plan (Reference: D26/7536)
- ICT Strategic Plan 2026-2031 (Reference: D26/5757)
- Privacy Policy
- Data Breach Response Policy
- Essential Eight Maturity Model
- Local Government Council Members' Records

Legislation

- *State Records Act 2000*
- *Local Government Act 1995*
- *Local Government (Model Code of Conduct) Regulations 2021*

Associated documents

- Code of Conduct – Councillors
- Code of Conduct - Workers
- Records Management Procedures
- Data Breach Register.
- ICT Security Standards
- State Records Commission Retention and Disposal Schedules

Document control information	
Document Category	Governance
Document Title	Information Management and Information and Communications Technology (ICT) ICT Acceptable Use
Document ID	GOV29
Document Owner (position title)	Executive Manager Finance and Corporate Services
Author (position title)	Executive Manager Finance and Corporate Services
Initial Council Adoption *(including Date and Resolution No.)*	2 April 2026 (Council Resolution OCM156/07/26)

Document control information	
Last Council Review *(including Date and Resolution No.)*	2 April 2026 (Council Resolution OCM156/07/26)
Date of Approval	2 April 2026 (Council Resolution OCM156/07/26)
Approving authority	Council
Absolute or Simple Majority Decision:	Absolute Majority
Access restrictions	Nil
Date Published	30/07/2026
Date of Next Review	Mandatory annual review aligned with the annual financial audit cycle.