



SHIRE OF KONDININ

ICT Acceptable Use Policy

Policy Name	ICT Acceptable Use Policy
Responsible Department	Corporate Services
Policy Owner	Chief Executive Officer
Applicable To	All Employees, Elected Members, Contractors, Volunteers and Visitors

1. Objective

The Shire of Kondinin is committed to the responsible, secure and lawful use of its corporate information and communications technology (ICT) facilities. This policy sets out the conditions for acceptable use of all Shire ICT facilities, including the network, computer systems, internet and email access, corporate systems and hardware.

The policy applies to all users, including elected members, and aims to:

- protect the Shire against cybersecurity risks, data breaches and legal liability;
- ensure ICT resources are used efficiently and for their intended purposes;
- preserve the confidentiality and integrity of Shire information; and
- ensure compliance with applicable legislation governing privacy, surveillance and communications.

This policy should be read in conjunction with the Shire's Social Media Policy.

2. Scope

This policy applies to all employees, elected members, contractors, volunteers and visitors (collectively referred to as users) who access or use the Shire of Kondinin's ICT facilities at any time, whether on Shire premises or remotely.

It applies to all Shire-owned devices and systems, and to personal devices used to access Shire networks or systems. All users are bound by this policy from the point at which they are granted access to Shire ICT facilities.

3. Definitions

Authorised User – Any person who has been granted authorised access to the Shire's ICT facilities.

Elected Member – A Councillor or the Shire President elected under the Local Government Act 1995 (WA).

Email – The Shire's Microsoft Outlook, Outlook Web Access, or any Shire email system synchronised to a computer or mobile device, whether Shire-owned or personally owned.

ICT (Information, Communications and Technology) – Includes, but is not limited to, mail, telephones, mobile phones, voicemail, SMS, email, intranet, computers, tablets, printers, multi-functional devices, scanners and other electronic devices owned or managed by the Shire.

Malware – Malicious software designed to cause damage or perform unwanted actions on a computer system, including spyware, worms, viruses and Trojans.

Network Access – Connectivity from any device to Shire-managed ICT infrastructure, including local and remote network servers.

Prohibited Material – Content that could reasonably be regarded as pornographic; contains offensive language, cruelty or violence; is illegal, defamatory or discriminatory; breaches copyright; promotes terrorism or encourages terrorist acts; or contravenes the Shire’s values and policies.

4. Legal Framework

- Copyright Act 1968 (Cth)
- Criminal Code Act 1995 (Cth) - Part 10.7 (Computer offences)
- Local Government Act 1995 (WA)
- Local Government (Model Code of Conduct) Regulations 2021 (WA)
- Privacy Act 1988 (Cth) - to the extent applicable, including tax file number information, Commonwealth-related obligations, or dealings with APP entities.
- Privacy and Responsible Information Sharing Act 2024 (WA) - primary privacy framework for the Shire from 1 July 2026, including the Information Privacy Principles; serious information breach notification obligations commence on 1 January 2027.
- Spam Act 2003 (Cth)
- State Records Act 2000 (WA)
- Surveillance Devices Act 1998 (WA)
- Telecommunications (Interception and Access) Act 1979 (Cth)

5. Policy Statement

General Use of ICT Equipment

Shire business records, communications and information created, sent, received or stored using Shire ICT facilities are Shire records and must be managed in accordance with the State Records Act 2000, the Shire’s Recordkeeping Plan, and applicable privacy, confidentiality and access to information requirements.

Users should not store private personal material on Shire ICT systems. The Shire will take reasonable steps to protect personal information held on its systems. Users acknowledge that Shire ICT systems may be accessed, monitored, audited, preserved or disclosed where lawful and reasonably required for business, security, compliance, legal, audit, recordkeeping or operational purposes.

The Shire may monitor, access, audit or review use of Shire ICT facilities where lawful and reasonably required for security, operational, compliance, audit, legal, misconduct, recordkeeping or business continuity purposes.

Monitoring must be undertaken in accordance with applicable law, including privacy, surveillance, telecommunications interception and access, and records legislation. This Policy does not authorise unlawful interception of communications or unlawful recording of private conversations or private activities.

Personal Use

A reasonable degree of personal use of Shire ICT assets is permitted. Personal use must be undertaken before or after contracted work hours or during authorised breaks; must be limited and brief, avoiding excessive downloads or data transmission; and must be consistent with all other provisions of this policy. Where there is uncertainty about acceptable personal use, employees should consult their line manager and elected members should seek guidance from the CEO.

Security and Confidential Information

All information stored on Shire corporate systems is to be treated as confidential. Users must not share or distribute Shire information without appropriate authorisation. Passwords and accounts must not be shared. Users are responsible for the security of their own passwords and must change them in accordance with ICT guidance. All devices connected to Shire systems must run approved and current anti-virus software. Users must report any malware warnings to the CEO or responsible officer immediately.

Email and Communications

All outgoing Shire emails must include the approved email signature and disclaimer as specified by the Shire's style guide. The following are not permitted using a Shire email address:

- sending or forwarding unsolicited messages, junk mail or chain communications;
- harassment via electronic means;
- using Shire networks to generate unsolicited communications;
- sending confidential Shire information to external parties or personal email addresses;
- communicating in a manner that could damage the Shire's reputation; or
- making statements on behalf of the Shire without express authority.

Personal email accounts must not be used for Shire business, except in an unavoidable emergency or where expressly authorised. Where a personal account is used in such circumstances, the user must ensure the communication is captured into the Shire's recordkeeping system as soon as practicable.

Remote Access

Users with remote access must ensure their device is secure and remains under their complete control. All remotely connected devices must have current anti-malware software. Users should avoid public access terminals when connecting to Shire systems. When connected remotely, all Shire rules and obligations apply equally.

Personal devices used to access Shire systems may be subject to Shire security requirements, including password protection, multi-factor authentication, device encryption, approved applications, remote access controls and removal of Shire data when access is no longer authorised.

Unacceptable Use

The following are prohibited at all times: engaging in any illegal activity using Shire ICT systems; accessing or distributing Prohibited Material; violating intellectual property rights; installing unlicensed software; introducing malware into Shire systems; sharing passwords or allowing others to use personal accounts; and using Shire equipment for private commercial work or making fraudulent offers.

The following require express role-based authorisation:

- conducting security testing;
- intercepting network data;
- attempting to bypass Shire network security;
- interfering with another user's account; or
- using systems in a way that degrades network performance.

Removal of Access or Amendment of Access

ICT access must be removed or amended promptly when:

- (a) an employee's employment ends;
- (b) an elected member leaves office;
- (c) a contractor's engagement ends;
- (d) a volunteer or visitor no longer requires access;
- (e) a user changes role; or
- (f) access is no longer required for an authorised Shire purpose.

The relevant manager, contract manager, executive manager or responsible officer must notify the ICT provider as soon as practicable so that access can be removed or amended.

Mobile Phones and Electronic Devices

Some employees and elected members may be provided with a Shire mobile phone, tablet or other electronic device where necessary. All such devices remain the property of the Shire and users must comply with this policy.

Privacy & Personal Information

The Shire is subject to the Privacy and Responsible Information Sharing Act 2024 (WA). Users must collect, use, access, disclose, store and dispose of personal information only for authorised Shire purposes and in accordance with the Information Privacy Principles, the Shire's privacy procedures, records requirements and any lawful direction.

Users must not copy personal information to personal email accounts, personal cloud storage, portable media or personal devices unless expressly authorised and subject to appropriate security controls.

Any suspected unauthorised access, use, disclosure, loss or compromise of personal information must be reported to the CEO or responsible officer immediately.

From 1 January 2027, the Shire will be required to comply with the serious information breach notification scheme under the Privacy and Responsible Information Sharing Act 2024 (WA).

Breach of this Policy

For employees: This policy constitutes a lawful instruction. Any breach may result in disciplinary action up to and including termination of employment. The Shire may also temporarily block or remove ICT access.

For elected members: Alleged breaches may be dealt with in accordance with the Local Government Act 1995, the Local Government (Model Code of Conduct) Regulations 2021, the Shire's Code of Conduct for Council Members, Committee Members and Candidates, and any applicable Council resolution concerning access to Shire ICT facilities.

The temporary suspension or restriction of ICT access may be used as an administrative control to protect Shire systems, information security, privacy or business continuity. It is not, of itself, a disciplinary sanction.

6. Roles and Responsibilities

Council: Responsible for adopting and reviewing this policy and applying the Shire's Code of Conduct framework where relevant to elected member use of Shire ICT facilities.

Chief Executive Officer: Responsible for overall administration of this policy; approving exceptions; ensuring ICT, privacy, cybersecurity and records obligations are managed; and taking action to protect Shire ICT systems, including restricting access where necessary.

Responsible Officer / ICT Manager / ICT Service Provider: Responsible for implementing technical controls, monitoring network activity, responding to security incidents, advising on password management and device security, and reporting incidents to the CEO.

Line Managers: Responsible for ensuring employees are aware of and comply with this policy, and escalating breaches to the CEO.

Executive Managers: Responsible for advising the ICT provider of the termination or resignation of a member of staff from their department, so that the staff member's access to Shire ICT facilities can be removed in a timely manner.

All Users: Responsible for using Shire ICT facilities only in accordance with this policy, reporting security incidents or data breaches immediately, and seeking guidance where uncertain.

7. Review

This policy will be reviewed every four years, or earlier if required by changes to relevant legislation, significant changes to Shire ICT systems, or a significant security incident. This policy was last reviewed to reflect the commencement of the operative provisions of the Privacy and Responsible Information Sharing Act 2024 (WA) on 1 July 2026.

Document References & Information	
Legislation	Copyright Act 1968 (Cth); Criminal Code Act 1995 (Cth) Part 10.7; Local Government Act 1995 (WA); Local Government (Model Code of Conduct) Regulations 2021 (WA); Privacy Act 1988 (Cth) to the extent applicable; Privacy and Responsible Information Sharing Act 2024 (WA); Spam Act 2003 (Cth); State Records Act 2000 (WA); Surveillance Devices Act 1998 (WA); Telecommunications (Interception and Access) Act 1979 (Cth).
Regulation	
Local Law	
Shire Policy	Code of Conduct for Elected Members; Code of Conduct for Employees; Disciplinary Directive; Social Media Policy
Procedural	ICT Acceptable Use Acknowledgement Form; Data Breach Response Procedure; Remote Access Request Form
Related Sources	WALGA ICT Guidance; Office of the Australian Information Commissioner - Notifiable Data Breaches guidance; WA Information Commissioner - Privacy and Responsible Information Sharing Act 2024 guidance (from 1 July 2026)
Policy Owner	Chief Executive Officer
Risk Rating	Low to Medium

Document Control				
Date	Version	Reason for Modification	Resolution Reference	Next Review
12.7.2026	1	Amended Policy to include the PRIS Act.	OCM/26/089 22.7.2026	July 2030