Information Technology

POLICY

Policy Version 2.0
Category: Management
Adopted: November 2025

Information Technology Policy & Procedure

Purpose

This policy sets out how Winton Shire Council's information technology resources are to be used and protected. It establishes clear expectations for staff behaviour, while ensuring Council systems remain secure, reliable, and available to support operations and community services.

Scope

This policy applies to all Councillors, employees, contractors, volunteers, and third parties who use Council IT systems, data, or devices, whether on Council premises or remotely.

Definitions

Term	Definition
CEO	The person appointed to the position of Chief Executive Officer under the Local Government Act 2009, and anyone acting in that position.
Council	Winton Shire Council
Employee	Includes any person employed by Council and persons providing services to or on behalf of Council, including Elected members.
Email	A service that enables people to exchange document or material in an electronic format.
Hack	To gain access into another's computer system or files by illegal or unauthorised means.
Information Technology (IT)	An umbrella term covering websites, technology, applications, or tools that enable an exchange of dialogue between organisations, communities and individuals. IT may include but is not limited to: • Computers – desktop and laptops • Mobile devices – phones and tablets • Internet – corporate and public, physical and wireless • Software – email, content creation
Internet	A global research, information and communication network providing services such as access to information, file transfer and electronic mail.
Material	Includes data, information, text, graphics, animations, speech, videos, photos, maps and music or other sounds, accessible electronically, including any combination or selection of any of these.
Standard Operating Environment (SOE)	Refers to the specific combination of computer hardware and software configuration on Council computers.

Policy Statement

Winton Shire Council is conscious of the need to handle Council information in a way that promotes and maintains the public's trust and confidence in the integrity of Council whilst maintaining privacy and confidentiality under the corresponding legislative Act's.

Council holds information about a range of matters relating to Council business and information relating to private individuals and commercial entities. Council acknowledges that to minimise risks to the Council and residents, Council must manage all IT devices in a way to preserve the privacy and confidentiality of information held by Council to the fullest extent possible.

Responsible Use

Council provides IT resources for business purposes. Limited personal use is permitted, provided it does not interfere with work duties, create additional cost, or breach this policy. Users must act lawfully, ethically, and in line with Council's Code of Conduct. Council may monitor IT systems to protect its assets, and users should have no expectation of privacy.

Security & Access

Access to Council systems is provided on the principle of least privilege – meaning users are only granted the minimum level of access require to perform their duties. All access is based on business need and may be withdrawn at any time. Users are responsible for protecting their accounts and devices. Passwords must be at least eight characters long, unique, and never shared. Multi-factor authentication (MFA) must be used wherever supported. Devices must be locked when unattended and kept up to date with security patches. Any loss or theft of equipment must be reported immediately.

Authorised Systems & Records

Council information must only be stored and managed in authorised Council systems. Staff must not store Council data in personal cloud accounts (e.g. Google Drive, Dropbox) or sign Council up for third-party platforms without IT and management approval.

All information created or received in the course of Council business is a public record and must be managed in accordance with the Public Records Act 2002, Information Privacy Act 2009, and Council's Records Management Policy.

Cybersecurity

Council aligns its practices with the Australian Cyber Security Centre's Essential Eight and the NIST Cybersecurity Framework. This means Council actively patches systems, restricts administrative privileges, backs up data, and uses MFA. While the IT team manages technical controls, users play a vital role by reporting suspicious emails, avoiding unapproved software, and promptly raising any security concerns.

Artificial Intelligence

Council supports the responsible use of Artificial Intelligence (AI) to improve productivity and services. AI tools must comply with Council's data governance requirements, including ensuring that data is stored in Australia. Microsoft Copilot is the approved platform for general language models. Other AI platforms may only be used with explicit IT and executive approval.

Access & Equipment Care

Access to Council's systems will only be granted once the appropriate access request has been authorised.

Council IT equipment remains Council property. Employees are responsible for the care of their issued equipment and must report any damage immediately to IT. All devices must be returned when employment ends.

Council-issued mobile devices are provided for business purposes only. Personal use is not permitted, and employees may be held responsible for any excess charges, including those incurred during periods of leave.

Users should be aware that Council data and email messages, even if marked confidential, may be disclosed in legal proceedings, information access requests, or as required by law.

Copyright & Intellectual Property

The copyright of artistic, literary, dramatic, or musical works created by Council employees in the course of their duties is owned by Council, unless otherwise agreed.

Employees must not create, copy, or distribute unauthorised copies of Council data, information, or intellectual property for non-Council purposes. Staff must comply with the Copyright Act 1968 and other intellectual property laws. Most materials on the internet, including text, graphics, and sound, are protected by copyright and cannot be used without permission. Breaches may result in disciplinary action and legal liability.

Device Procurement & Security

All IT devices must be purchased through Council's procurement process and must pass through the IT department before being issued. The IT department will register devices, apply baseline security controls, and ensure they are ready for safe use. Devices must not be altered or reconfigured without IT approval.

Compliance

Failure to comply with this policy may result in disciplinary action and, where unlawful activity is involved, referral to law enforcement. Exceptions to this policy must be approved by the Chief Executive Officer or delegate.

Communication

- Councillors and all Council employees will have access to this policy.
- Councillors and all Council employees will be provided with opportunities to be involved in the review of this policy.
- Council employees will be provided with information from this policy at the time of employment and orientation.
- Changes/amendments made to this Policy document will be communicated to all Councillors and Council employees.

Enforcement

Non-compliance with this policy could place Council in breach of both the **Local Government Act 2009** and/or the **Information Privacy Act 2009**. It is important to note that non-compliance with this policy/procedure by an individual could lead to personal liability and/or criminal prosecution.

The failure of any Council employee to comply with this policy in its entirety may lead to:

- Refresher or further training,
- Performance management, or
- Modification or termination of employment.

Related Council Documentation

- Code of Conduct for Employees

- Councillor Code of Conduct
- Social Media Policy
- Cyberbullying Policy
- Privacy and Confidentiality Policy

Legislation, recognised Authorities and other sources

- Local Government Act 2009
- Local Government Regulation 2012
- Copyright Act 1968 (Federal)
- Right to Information Act 2009
- Information Privacy Act 2009
- Crime and Corruption Act 2001
- Human Rights Act 2019
- Invasion of Privacy Act 1971
- Office of the Information Commissioner

CEO Discretion

Where applicable, the CEO can apply their discretion as to the enforcement of the requirements outlined in this policy and any requests for variations to this policy.

Review of Policy

This policy remains in force until amended or repealed by resolution of Council. This document will be reviewed biannually or as required.

Record of amendments and adoptions

Date	Version	Reason for amendment	Date adopted by Council & Resolution Number
November 2021	1.0	Preparation for Council Adoption	17 December 2021
November 2025	2.0	Updates to the policy to align with new legislation	20 November 2025; 13.6 2025/167