WINTON SHIRE COUNCIL
INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY (IT) POLICY & PROCEDURE

Table of Contents

PURPOSE

The purpose of this Winton Shire Council Information Technology Acceptable Use Policy and Procedure is to:

- Clearly identify the parameters when using Winton Shire Council's information & communication technologies
- Outline the process for using Winton Shire Council's information & communication technologies
- Protect the interests, intellectual property, and IT assets of Winton Shire Council

SCOPE

This Information Technology Acceptable Use Policy applies to Councillors and all Council Employees of Winton Shire Council (WSC) who use information and communication technologies for or on behalf WSC.

This document provides direction on the acceptable use of WSC's information and communication technologies, and personal use of WSC's information and communication technologies.

Note: Personal use of personal information and communication technologies does not apply to this policy.

DEFINITIONS

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

Director – A person appointed in a Department Director level position

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.

PROCEDURE

Acceptable Use

The Council information technology (IT) infrastructure and services are primarily for Council business use and must be used in accordance with legislative requirements and the guidelines set out in this Policy.

SOE Access

Employees will only be granted access to Council's operating environment once a ***Network Access Request Form*** has been completed, and authorisation given by the appropriate department Director.

Personal Usage

Employees may be permitted to use Council IT equipment and infrastructure for private purposes - only where such use is open, accountable, and transparent. Private use must always be appropriate and lawful and not interfere with employee's capacity or ability to perform their respective duties.

Passwords

Passwords are an employee's electronic authorisation used to gain access to Councils IT systems. Employees are responsible for the security and regular changing of their password(s).

Passwords are required to adhere to the following rules:

- Must be at least 8 characters in length
- Must contain at least one number
- Must contain at least one upper case letter
- Must not contain easily guessable words or phrases (i.e. Winton, 4735, Password)
- Required to be changed once a month

Employees are required to take reasonable precaution to ensure that their password is not known by any other party, this includes not writing the password down in an easily accessible location.

Employees must not disclose their password(s) to anyone however employees may be required to disclose their password to a Director or IT staff, in this instance the employee may request that their password be changed before disclosing.

Identity

No email or other electronic communication may be sent for or on behalf of Council which conceals or attempts to conceal the identity of the sender.

All Council email correspondence is required to include the standard Council email signature, which **must** include the following:

- Employee Name

- Employee Title/Position
- Employee email address
- Council Emblem & name
- Council primary contact number (no direct extensions to be advertised)
- Council mobile number (if employee has been issued a mobile phone)
- Council Postal address
- Links to Council websites (Corporate & Tourism)
- Confidentiality clause

The only exception is where it is intended to keep the identity of the sender anonymous, such as position or purpose related mailboxes (i.e. HR, Jobs, Info, Tenders), which may omit an Employees name.

Email Usage

Council email access is provided to employees on an "as required" basis. Council provided email is strictly to be used for Council business purposes only.

Employees must exercise care and discretion with electronic communication such as tenders, contracts, confidential agendas, minutes, and reports.

Email messages are perceived to be instant in nature and instantly disposed of, however all emails sent and received from Council email are backed up and stored indefinitely, regardless of any accidental or deliberate deletion.

Improper statements can give rise to liability, personally and for Council. Employees must operate on the assumption that messages may be sent to, forwarded to, transmitted or printed by someone other than the intended recipient.

Employees must be aware that email messages, even if expressed to be confidential, may be disclosed in legal proceedings, Freedom of Information requests, or as required by law.

Employees should follow 'best practice' when using Council email, so as not to cause Council disrepute. Best practice examples include:

- Subject line should be clear and concise and not contain the body of the email
- Contents of the email should be lawful and free of error
- All sent emails must contain the standard Council signature

Security

To increase data security, Council computers are configured to lock access after a period of inactivity. After this time employees will be required to re-enter their passwords to re-gain access. Employees must not attempt to circumvent this security function.

Employees are required to lock their computers when leaving their desk for extended periods of time. Employees found to consistently leave their computer unsecured may be subject to disciplinary actions.

Employees must not attempt to gain access to another employee's user account, whether by knowing or guessing another employee's password or by other methods. Employees found to attempt to hack Council IT systems may be subject to disciplinary action.

Unknown USB storage devices are a high risk to Council data security. Employees must not attach unknown USB devices to any Council IT systems, this includes but is not limited to, USB storage devices containing files or material required to be printed by a member of the public, and personal Employee USB storage devices.

Remote Access

Employees may be authorised to access Councils network from a remote computer. Remote access may be granted on an "as required" basis only when required to work away, under authorisation from the CEO or appropriate department Director.

Employees authorised for temporary remote access shall be issued with a secure Council laptop to be used for Council business only, which must be returned at the end of the authorisation period. Employees should not store data on the laptop provided, and should assume that any data stored will be removed upon return.

The following employee positions may be issued with a Council administered laptop for the duration of their employment:

- CEO, Directors and Elected Members
- Managers - (Asset Manager, Works Manager, Senior Finance Manager, Community Health Manager, Parks & Facilities Manager, Human Resources Officer)

Laptops issued are to be used for Council business only. Under no circumstances is an employee to install software, modify configuration settings, or provide use of the issued laptop to anyone but Council IT staff. An employee issued with a Council laptop may be held responsible for any unlawful or unauthorised activity conducted on a Council issued laptop.

Exceptions may be made for companies which have entered into an agreement with Council for managed services that require frequent remote access. These companies shall be liable for any damage or data loss caused as a result of their remote access.

Employees found to be accessing Council IT systems remotely from an unauthorised computer or device may be subject to disciplinary action.

Under no circumstances are employees to grant remote access to a Council IT System to any persons via TeamViewer or any other method unless authorised to do so by Council IT staff. Employees found to allow unauthorised remote access to Council's network may be subject to disciplinary actions.

Document Management - InfoXpert

Council utilise InfoXpert as a ***document management system***. Employees required to use Council computers to perform their duties will be granted a "user workspace" inside InfoXpert.

Employees with access to InfoXpert are required to store all Council documents and Council business related emails in InfoXpert.

Data Storage

Employees will be granted access to Council data resources via mapped network drives on an "as required" basis. Authorisation to access a mapped network drive is to be granted or denied via the Network Access Request Form, with approval from the appropriate Director.

Employees may be granted access to a 'Z' drive, this is the only location that employees may store data that may be of a personal nature. All other network drives and data storage locations are to be used for Council business only.

Employees must not store unlawful content on Council IT systems. Council IT staff may monitor data stored on Council IT systems and infrastructure, and report findings to the CEO.

Hardware Care

Employees must not interfere with the physical configuration (i.e. placement, cabling, etc.) of Council IT systems including but not limited to, computers, printers, desk phones, power, and data. Any required configuration changes are to be authorised by IT staff prior to any changes being made.

Employees are responsible for the care of their Council IT equipment, and may be held accountable for any physical damages that may occur. Employees must report any physical damage to Council IT equipment to IT staff immediately.

Employees should turn off their computers at the end of each workday, unless otherwise directed by Council IT staff for the purpose of maintenance.

Mobile Devices

Dependant on positional requirements, employees may be issued with a mobile device (i.e. Mobile phone, tablet) to assist with performing their duties. The type of mobile device issued will depend on the requirements of the employee's position.

The employee roles that may be issued a mobile device are:

- CEO, Directors
- Managers (Asset Manager, Works Manager, Senior Finance Manager, Community Health Manager, Parks & Facilities Manager, Human Resources Officer)
- Officers that are directed to carry a device as part of their role

Employees are responsible for the care of the mobile device issued and may be held accountable for loss or damages caused. The mobile device must be carried by the Employee at all times during hours of employment and must not be forwarded or redirected to a personal mobile device.

Employees are not permitted to use a Council issued mobile device for personal use. Employees found to use a Council issued mobile device for personal use may be held accountable for any excess charges relating to that personal use.

If an Employee incurs excess usage charges on a Council mobile device whilst on leave or otherwise not performing duties related to Council business, that employee may be held accountable for those excess charges.

Upon an Employees termination, all issued IT devices must be returned to Council.

IP Telephony

Dependant on positional requirements, Employees may have a Council desk phone configured in their workspace. These desk phones are to be used for Council business only.

Employees should limit publicising their direct dial extension numbers and should direct contact to Council's primary contact number when possible.

Employees are responsible for the care of their desk phones, and any damages or faults must be reported to IT staff.

BYOD – Bring your own device

Council does not support the use of BYOD laptops.

Depending on position requirements, Council may reimburse employees up to 100% of their monthly phone charges for use of their personal mobile devices to perform Council duties. Employees may be required to produce evidence of their monthly phone costs. This would be subject to CEO/Director approval deeming that the device is necessary for the duties needed by the employee's role.

Personal laptops and mobile devices may only be connected to Council's IT infrastructure under the authorisation of Council IT staff or CEO/Directors.

Internet Use

Council internet is intended to be used primarily for Council business, though employees are permitted to access the internet for personal use where that personal use is lawful and does not impact the employee's ability or capacity to perform their duties.

Council internet usage is monitored by IT staff to determine both the appropriateness of the content being viewed, as well as the impact the usage may have on Council operation due to data and bandwidth usage. Council IT staff may report on employee internet usage to the CEO/Director if required.

Council have content filtering active on Council's internet service, used primarily to block malicious, inappropriate, or unlawful content. If an employee cannot gain access to a website that is required to perform their duties, due to content filtering, they may contact Council IT staff to request that the restriction be removed.

Wi-Fi Access

Council operate and maintain two separate wireless networks in varying Council buildings. One free for public usage under the wireless identifier ***Outback Telegraph***, the other is a corporate wireless network that connects directly to Councils IT systems and infrastructure under the wireless identifier *Winton Shire Council*.

Councils public wireless network is not secured by a wireless key and has speed limitations and restrictions in place to enable a fair service for all users. Employees are free to use the public wireless network in a lawful manner, provided it does not impact their ability or capacity to perform their duties.

Councils corporate wireless network is secured by a wireless key and is to be accessed by Council employees from authorised devices only. Authorisation can be granted to an employee using the **Network Access Request Form**, provided the employee has reasonable requirement to use the wireless network and has been issued a Council mobile device.

Visiting guests of Council that require unrestricted wireless internet may be granted access to Councils hidden guest wireless network. If a guest requires wireless internet access, a Council employee may request the access details from Council IT staff.

Software Configuration

Under Councils SOE, all Council IT equipment should have the same software packages installed. Exceptions may be made to the Council SOE where specific software is required for specific positions, these exceptions will be made at IT staff discretion after assessing the requirements.

Employees must not attempt to modify or install software on any Council IT system. If software not currently part of the SOE is required, Employees may contact Council IT staff to request that the software be installed, Council IT staff will review the request and approve or deny the request if appropriate and compatible with Councils IT systems.

Employees must not attempt to alter the configuration of any Council IT systems. If configuration changes are required, employees may request the change by contacting Council IT staff.

Malicious Software Protection

Council IT systems are protected from malicious software protection through the implementation of a number of layers of protection:

- Incoming & outgoing email filtering and inspection
- Internet content filtering & firewall
- Local antivirus/malware software

While Council's protection methods are effective in preventing most malicious software infections, employees must be cautious when opening emails and files from unknown or suspicious sources. Employees are encouraged to contact IT staff when they suspect a possible threat of infection.

Printing

Employees are encouraged to assess requirements before printing large or high-volume documents. Where possible, employees should print in greyscale to the high-volume photocopiers located in each Council building. Employees should refrain from using smaller desktop printers unless necessary.

Employees are responsible for replacing and ordering consumables for printers using the contact details located on each printer, Council IT staff may assist when required.

Visitors and members of the public that request to print material must be directed to email the file to a Council employee for printing. This ensures the file is inspected and scanned for malicious code by Council's email server.

Visitors and members of the public that request to print material but do not have the ability to email the file to a Council employee, must be directed to print from the publicly accessible computers available for use at the **Winton Library**. Under no circumstances should a Council employee attach an unknown USB storage device to Council IT Systems for the purpose of printing.

IT SUPPORT MATRIX

When an issue with Council IT systems or infrastructure is identified, an employee is to submit a support ticket to Council IT staff via the Council IT support portal http://support.winton.qld.gov.au. If an Employee is unable to submit a support ticket due to the nature of the issue, they may contact IT staff directly.

Council IT staff will assess each issue identified and attempt to respond to issues based on the following priority matrix:

	LOW	NORMAL	HIGH	URGENT
SEVERITY	Hindrance to the work of an individual user and/or a work around is available.	Interruption to the work of an individual user and no work around is available.	Interruption to critical business functions affecting an individual user and no work around is available.	Interruption to critical business function affecting multiple users and no work around is available.
Expected Response	7 days	2 days	1 day	4 hours

Note: The response times listed are indicative only and will be assessed per incident.

CONFIDENTIALITY

Employees should perform their duties under the assumption that all data stored on Council IT systems is accessible by IT Employees and the CEO upon request and may be reported on if required.

Employees must be aware that data and email messages, even if expressed to be confidential, may be disclosed in legal proceedings, Freedom of Information requests, or as required by law.

Refer to Council's Privacy and Confidentiality Policy.

COPYRIGHT

The copyright over artistic, literary, dramatic or musical work authored by WSC employees whilst carrying out work duties is owned by the WSC as per the Copyright Act 1968 (s35) unless by prior arrangement.

Under no circumstances is a Council employee to replicate unauthorised copies of Council data, information, or Intellectual Property for purposes other than Council business. Employees found to be doing so may be subject to disciplinary action.

Employees are required to adhere to the requirements of copyright legislation. Intellectual property rights apply to most material on the internet, including text, graphics, and sound. Employees must not assume they can reproduce, print, transmit, or download material to which they have access. Usage of any material should comply with copyright legislation, as any material reproduce outside permitted uses or without the permission of the owner may result in litigation action against Council.

UNLAWFUL ACTIVITY

Employees must not conduct or be party to any unlawful activity while using or through the use of Council IT systems. Any unlawful activity found to occur will be reported directly to the CEO and appropriate law enforcement agencies.

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	**REVISION NO**	**REASON FOR AMENDMENT**	**ADOPTED BY COUNCIL**
November 2021	V1.0	Preparation for Council Adoption	17 December 2021