ICT Acceptable Use Policy

Policy Number	A8
Responsible Officer(s)	Chief Executive Officer; Manager People & Governance.
Policy Adopted	October 2023
Next Review Date	October 2027
Minutes reference	2023/10-07
Applicable Legislation	*Privacy Act 1988* (Cth); *Australian Privacy Principles; Local Government Act* (SA) *1999; State Records Act* (SA) *1997; Spam Act (*Cth) *2003; Surveillance Devices Act* (SA) *2016; Equal Opportunity Act* (SA) *1984; Copyright Act* (Cth) *1968.*
Related Policies	Cyber Security Governance Policy; Information Privacy Policy; Records Management Policy.
Related Procedures	Data Breach Response Plan; Data Breach Response Checklist.

1. POLICY PRINCIPLE

The purpose of this policy is to provide guidelines for the acceptable use of Council Information and Communication Technology (ICT) assets by Council Members, employees, contractors and volunteers.

2. POLICY OBJECTIVE

- Support the safe and effective use of Council ICT assets
- Control risks associated with cyber security threats to Council ICT assets
- Protect the privacy of personal information
- Prevent inappropriate and unlawful use of ICT assets

3. DEFINITIONS

ICT Assets	All electronic devices provided or made accessible by Council. This includes mobile phones, tablets, laptops, desktop devices, software applications (local, external, cloud), Internet services, social media, communications networks, servers, storage media and security systems.
Council Information	All Council information that is electronically stored whether on local devices or external systems including on cloud based systems.
Private ICT Assets	Privately owned devices such as phones and laptops that may be used to access, store or process Council information.

4. POLICY DETAIL

This policy applies to Council Members, Council Employees, ICT providers to Council, Contactors, Volunteers and any other person who is provided access to Council ICT assets.

4.1 Standards

Council aligns its Cyber Security Governance Policy with the following as applicable to the Council context:

- Australian Cyber Security Centre, Information Security Manual, 10 March 2022 and subsequent revisions.
- International Standard ISO/ IEC27001:2015 Information Security Management.

4.2 Related Wakefield Regional Council Policies and Procedures

- Cyber Security Governance Policy, October 2023
- Data Breach Response Plan, October 2023
- Data Breach Response Checklist, October 2023
- Information Privacy Policy, January 2023

4.3 Roles and Responsibilities

All users of ICT assets must comply with this policy.

The Senior Leadership Team is responsible for implementation of this policy, monitoring compliance and managing non-conformance.

The Manager People and Governance is responsible for monitoring overall effectiveness of this policy and its ongoing improvement.

4.4 Use of ICT Assets Encouraged

The use of Council ICT assets for official purposes is actively encouraged and necessary to achieve the goals and objectives of Council.

4.5 Offensive Unlawful and Illegal Behaviour

Council ICT assets must not be used to engage in offensive, unlawful or illegal behaviour including but not limited to:

- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language.
- Recording telephone conversations unless authorised under the *Surveillance Devices Act* (SA) *2016*.
- Intentionally accessing, sending, receiving, storing, or printing pornographic, racist, sexist, or otherwise discriminatory, or objectionable material.
- Cyber bullying.
- Discriminating against persons in contravention of State or Federal laws.
- Breach of copyright laws.
- Electronic Spam.

4.6 Commencement and Cessation of Access

All persons requiring access to ICT assets must agree to comply with this policy as a condition prior to being granted access. A copy of the agreement shall be retained by Council.

Ceasing Council Members, employees, contractors and volunteers must return all ICT assets and Council information and continue to comply with any ongoing requirements of this policy.

Persons whose authorisation to use ICT assets has ceased shall not access, or attempt to access, Council ICT assets.

Where ICT access is to be provided the following agreements require compliance with this policy:

- Employment agreement
- Contractor agreements
- ICT provider agreements
- Volunteer agreements

4.7 Mobile Devices

Mobile devices are valuable business tools and essential to the conduct of business. Mobile devices provided by Council are subject to the following requirements:

- Mobile devices are issued for official use. Private use is restricted to incidental and limited use only and may be subject to monitoring by Council.
- Mobile devices left unattended must always be locked. Mobile devices are configured to automatically lock after a period of inactivity.
- Mobile devices must not be left unattended in public locations or where the risk of theft is increased. Devices may be stored in a locked vehicle out of public view.
- Mobile devices are configured with an authentication passcode. The passcode must not be recorded or saved in a location where it could be accessed by another person. Passcodes must not be shared unless a shared device such as a vehicle tablet.
- Mobile devices must not be used in contravention of Australian Road Rules.
- Loss of a mobile device must immediately be reported to the Team Leader Community. Lost phones will be remotely wiped.
- Mobile device operating systems and anti-virus configurations must not be modified by users unless approved by the Communications & IT Officer.
- Users of mobile phones and tablets may load relevant applications from the Apple ‘App Store’ and Google ‘Play Store’ for official purposes.
- Only software applications approved by the Team Leader Community for official purposes may be loaded onto laptop devices.
- Users must apply mobile device operating system and application software changes as directed by Council in a timely manner. These may include critical security updates to be applied within a short timeframe.
- Council official records must not be permanently stored on mobile devices as these are not backed up. These should be stored in Council’s Electronic Document and Records Management System (“EDRMS”).
- Personal private information must not be stored on mobile devices.

4.8 Privately Owned Devices / Working Remotely

Privately owned mobile phones and tablets may be used to access Council systems with prior

approval of Team Leader Community.

These may be used to access the following systems for Council business purposes subject to the private device usage conditions below:

- Council Microsoft email and calendar accounts;
- SkyTrust;
- Geographic Information System.

The private device usage conditions are as follows:

- Devices must automatically lock within 30 seconds.
- Devices must be protected by a secure authentication system such as fingerprint or facial recognition) or a secure password or passcode (passcodes and passwords must not be shared).
- The device login account must be restricted to the Council user (e.g. staff member, contractor, ICT provider). No other user shall be able to access the account.
- Devices must use the latest available operating system and all supplier recommended security patches must be in place.
- Devices must be less than 5 years old or run the latest operating system if greater than 5 years.
- The user must not attempt to access Council systems if it is known or suspected that device security is compromised.
- For Apple and Android mobile devices the 'remote wipe' capability must be enabled by the user.
- Council information must not be stored permanently on privately owned devices.
- All Council records, apps, access must be permanently removed from the device when the device ceases to be used for Council business or when employment ceases.
- Private information of the user must not be stored on Council assets.

Access to other systems will be assessed on a case by case basis and subject to approval of the Manager People and Governance. Where private laptops and personal computers are authorised for use in addition to the above these shall have current anti-malware protection installed.

All requirements of this ICT Acceptable Use Policy apply when the approved private device is used for Council business.

Private devices are used entirely at the user's discretion, and Council does not accept any responsibility for any loss arising or associated with the use of the private device to access Council systems.

4.9 Passwords and Multifactor Authentication

Access to ICT assets is gained via login names and passwords. The user requirements for managing passwords are as follows:

- Passwords must not be shared;
- Passwords must meet complexity and length requirements specified by Council (enforced by its ICT systems);

- Passwords must not be recorded in a manner where they may be accessible to others;
- Passwords must be updated in a timely manner as directed by Council;
- Passwords must never be emailed.

Multifactor authentication details (e.g. one-time codes) must not be shared or disclosed.

4.10 Internet

Internet access may be provided for official purposes. Users should be aware that Internet filtering and monitoring systems have been implemented by Council.

Internet access must not be used for:

- Accessing objectionable (including pornographic or violent) or criminal material;
- Exchanging highly confidential or sensitive information;
- Creating, storing or exchanging information in violation of copyright laws;
- Gambling, gaming, conducting a business or conducting illegal activities;
- Playing electronic or online games;
- Downloading personal items such as videos and streaming services.

Personal usage of Internet access is subject to incidental and limited usage only. Personal private information must not be exchanged.

4.11 Email Security

Email is a major source of security risk but also an essential part of conducting Council business.

Council maintains a range of controls to protect from malicious email security threats. These include Spam filtering, email security software and 'multi factor authentication'. Nonetheless not all malicious emails can be 'blocked', and users will be exposed to malicious emails.

Email account hacking and account impersonation are common methods for cybercriminals to send fake invoices, phishing emails, or malicious attachments.

ICT users must maintain awareness and vigilance in managing email security including:

- Not opening suspicious messages from external sources e.g. unexpected messages, messages from a suspicious source, email addresses that don't appear correct.
- If a message seems suspicious, contact the person or business separately to check if they have sent the message. Use contact details you find through a legitimate source and not those contained in the suspicious message.
- Be especially cautious if messages are very enticing or appealing (they seem too good to be true) or threaten you to make you take a suggested action.
- If unsure, thinking carefully before clicking on links or opening attachments. Before you click a link (in an email or on social media, instant messages, other web pages, or other means), hover over that link to see the actual web address it will take you to (usually shown at the bottom of the browser window). If you do not recognise or trust the address, try searching for relevant key terms in a web browser. This way you can find the article, video or web page without directly clicking on the suspicious link.
- Taking care when sending emails to ensure they are addressed to the intended recipient

only. Particular care must be taken when sending emails to distribution lists and maintaining privacy.

- Maintaining awareness and acting on advice received from Council and its ICT providers in relation to email security and threats (as these are continually evolving).

Email must not be used for:

- Creating or exchanging messages that are offensive, harassing, obscene or threatening;
- Cyber bullying;
- To send unsolicited commercial electronic messages prohibited by the *Spam Act 2003*;
- Discriminatory behaviour.

Personal use of Council email accounts is limited to incidental and non-sensitive usage only. Council emails are official records and may be accessed by Council. Personal private information must not be exchanged via this usage.

Users of ICT asset acknowledge that Council may conduct simulated attack campaigns to test compliance and effectiveness of its email security policies.

4.12 Access to ICT Assets

Users must only access ICT assets as authorised. Access permissions will be set up for all users of ICT assets and removed on cessation of employment.

4.13 Removeable Media

Examples of removable media include USB drives, hard drives, and mobile phones.

Council recognises that the exchange of large amounts of data is necessary for many Council activities. The following requirements apply:

- Connection of non-Council USB devices and hard disks is prohibited. These devices represent a very high security risk to Council.
- The use of Council USB devices and portable hard disks is prohibited.
- Large files may be exchanged using Council provided secure enterprise grade cloud-based systems e.g. Dropbox.
- Where data is required to be extracted from a USB please contact the Manager People and Governance.
- Hard discs may be used by authorised Council ICT officers for offline backup storage. The backup hard discs must be registered and stored securely in a safe or other secure location.

4.14 Remote Working

Users working remotely, including from home, must comply with this ICT usage policy and ensure that ICT assets are kept physically secure within the work environment to the extent reasonably practicable.

4.15 Wireless Network Security

Users must not connect to public or unsecured public wireless (Wi-Fi) networks to gain access to Council systems. Council secure Wi-Fi (with passcode) may be used at Council locations and cellular mobile phone networks may be used at other locations. If travelling overseas special arrangements will be made.

4.16 Backups

Daily and weekly backups are automatically generated for all data stored on official Council 'drives' and all email accounts. Should data be lost this may be restored from backups.

4.17 Disposal of ICT Assets

Surplus ICT assets shall be securely disposed of by Council's ICT support provider or other agreed party and must include verification that all Council information has been securely wiped and that software licenses and other information has been removed. Users must not dispose of Council IT assets.

4.18 Personal Private Information

The storage of personal private information on ICT assets is subject to the Council's Information Privacy Policy.

4.19 Information Security Incidents

All information security incidents including known and suspected security breaches must be reported to the Communications & IT Officer immediately and all instructions followed.

Users are requested to record information where possible concerning the incident to assist investigation and recovery in accordance with the Data Breach Response Plan and Checklist.

4.20 Monitoring and Compliance

Council monitors compliance with this policy.

Breaches of this policy may result in investigation and/or referral to relevant external authorities. Users should be aware this may result in disciplinary, and/or civil, and/or criminal proceedings.

Council is required to report certain illegal activities to authorities and will cooperate fully with authorities in these matters.

5. REVIEW

This Policy shall be reviewed every 48 months, or more frequently if required by legislation or Council.

Document history:

Version	Adopted	Description of Change
1.0	October 2023	New Policy