INFORMATION SERVICES USAGE POLICY

01.15.04

1. BACKGROUND

The Policy for Information Services Usage was originally adopted by Weddin Shire Council (Council) on 20 August 2009 and has been reviewed on a further three occasions.

Information Services refers to the interconnected set of components used to collect, store, process and transmit data and digital information. This policy outlines the rules and restrictions around the usage of Councils Information Services systems.

Council has prepared this policy to develop a standard to which Council employees, Councillors, consultants, contractors, volunteers, work placement students or any other persons who use Council's Information and Communication Technology (ICT) assets and resources and is to be read in close conjunction with Council's Cyber Security Policy.

2. PURPOSE

Council's ICT assets including computers, network infrastructure, software applications, email, Internet and communication systems are a critical resource in the day-to-day running of Council's operations.

This document sets out to define the user's responsibilities, rules, standards and guidelines relating to the effective use of Council's ICT assets and resources and identifies sanctions that could be applied for any improper use of council's ICT assets.

3. POLICY OBJECTIVES

The objectives of this policy are to provide guidelines for the use of Council's ICT assets and resources, including:

- All Council owned devices including Desktops, Laptops, Tablets, and Phone.
- Personal devices that have been approved for use for Council operations.
- All network systems, applications and data.
- All corporate software applications.

Note: The Corporate Services Department can help to select and install other specialised applications as per Weddin Shire Council Cyber Policy 6.4.3 Software Installation. Support for application can be offered by the Corporate Services Department, who will reach out to third parties if required.

4. LEGISLATION

Council and its users have a responsibility to comply with relevant laws when using Council ICT assets and resources. Council must also comply with relevant legal provisions when monitoring or enforcing requirements set in the policy.

This policy relates to the following legislation:

- *Privacy Act 1988*
- *Security of Critical Infrastructure Act 2018 (SOCI Act)*
- *The Criminal Code Act 1995*
- *Local Government Act 1993*
- *Weddin Shire Council Policy For Records Management*
- *Weddin Shire Council Cyber Security Policy*
- *Weddin Shire Council Social Media Policy*
- *Weddin Shire Council Code of Conduct (as amended)*
- *Local Government (State) Award 2023- Disciplinary Procedures (as amended)*
- *Weddin Shire Council CCTV Workplace Surveillance*
- *Workplace Surveillance Act 2005 (NSW)*
- *Weddin Shire Council Work Health Safety Policy*

5. APPLICATION/SCOPE

This Policy applies at all times to Council employees, Councillors, consultants, contractors, volunteers, work placement students or any other persons who use Council's ICT assets and resources.

Use includes sending and receiving electronic communications including email and text, accessing the internet, accessing Council network, use of desktops, laptops, portable devices, and access and use of all applications and data.

The Policy must be read in conjunction with Council's Cyber Security Policy.

6. POLICY

6.1 Roles and Responsibilities

The following table outlines the roles and responsibilities of personnel. Noting that the position titles may change, however, the responsibilities remain the same.

Roles	Responsibility
The Elected Council	Council has the responsibility to consider draft local policies and the adoption of the local policy. This Policy also applies to Councillors and their own use of Council's ICT Resources.

Roles	Responsibility
General Manager	The General Manager is responsible for the overall control and implementation of the Policy.
Director of Corporate Services	The Director Corporate Services is responsible for updating the Information Services Policy in line with legislative amendments and/or reviewing and updating as appropriate. They are responsible for implementing the Policy and ensuring compliance.
Directors	The Directors are responsible for ensuring that their staff adhere to the requirements of the policy.
IT Officer/Team Leader Finance	The IT Officer and Team Leader Finance are responsible for the implementation of the Policy and the development of accompanying procedures.
MANEX	General Manager, Directors and HR Manager must be accountable for cyber security including risks, plans, reporting and meeting the requirements of the OLG Guidelines.
All Council employees, consultants, contractors and volunteers	All Council employees, consultants, contractors and volunteers are required to adhere to the Policy. as a user of the digital assets.
General Public	The general public must act in accordance with this policy and abide by any determination made as a result of this policy.

6.2 General Responsibilities

Council may provide a device in the form of a Desktop, Laptop, Tablet, or Mobile as an aid to staff to complete any tasks associated with their jobs. Users of Council’s ICT assets and resources, are required to:

1. Use the systems in the manner for which they are intended.
2. Follow Work Health & Safety Policy guidelines for the use of screen-based equipment.
3. Maintain mouse, keyboard, monitor and any other peripheral equipment and ensure they are in kept in good, clean condition.
4. Be wary of malicious files or Uniform Resource Locator (URL) any report suspected malicious files or URLs to IT.
5. Report any breaches of the policy to the relevant Team Leader/Manager or Director.

6. Agree to abide by these responsibilities by signing the attached User Agreement Form (as amended).

6.2.1 Prohibited Actions

Under NO circumstances should users:

6.2.1 Waste time on non-council business. Personal usage in excess of five (5) minutes during normal work time is considered to be wasting productive work time.

6.2.2 Allow other staff or any member of the public to access your personal computer (PC) or your PC login or email.

6.2.3 Solicit non-Council business for personal gain or profit.

6.2.4 Reveal or publicise confidential or proprietary information which includes, but is not limited to:

- 6.2.4.1 Financial information.
- 6.2.4.2 Council business, strategies, plans, databases and the information contained therein.
- 6.2.4.3 Council employee, client, ratepayer, resident or other community information.
- 6.2.4.4 Technical information.
- 6.2.4.5 Computer/network access codes.
- 6.2.4.6 Information about Council’s business relationships which you are not authorised to release, reveal or publicise.

6.2.5 Use any computers, software, Internet or email for any illegal purpose or to send any objectionable material that contains content that is defamatory, offensive, obscene or indecent in nature.

6.2.6 Perform any other inappropriate activities..

6.2.7 Visit Internet sites that contain offensive material.

6.2.8 Upload or download pirated software.

6.2.9 Attempt to install software without approval.

6.2.10 Send unsolicited mass marketing material.

6.2.11 Use any Council Device for gaming in or out of work hours.

Usage of any of Council’s computer systems may be monitored for compliance with these policies. Council reserves the right to carry out computer surveillance of any user at any such time that Council chooses without further notice to any user as outlined in the Cyber Security Policy 6.4.11 Computer Surveillance Records. Such auditing may form the basis of further investigation and subsequent disciplinary action.

6.3 Computer Network Responsibilities

Council may permit access to any or all of the computer networks to which council equipment is connected. Council may restrict levels of access to data. When you use Council's computers or network you should:

1. Manage your passwords appropriately.
2. Store all corporate information in Council's File Server. Data may be stored on Users device until completed and then added to the server under the appropriate location. In the event that data is stored on the individual user's device, this must be completed and added to the server under the appropriate location. Individual users are encouraged to operate from their U: drive.

6.3.1 Prohibited Computer Network Responsibilities

Under NO circumstances should users:

1. Have a password that is easily identifiable such as your name, initials, family name, etc.
2. Give your password to anyone else.
3. Use someone else's network logon account or allow someone to use your account.
4. Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
5. Attempt to install software that has not been approved for use by the relevant Director.
6. Examine, change, delete or use another person's files or output for which you do not have explicit authorisation to do so.
7. Store any offensive material on your PC or on the network data drive.

6.4 Email Usage Responsibilities

Council provides all personnel who have access to the network with an email account. This account is to be used for Council business. All email messages are considered records for all legal, fiscal, administrative, and historical purposes and remain the property of Weddin Shire Council. Council may monitor and audit email sent to and from the Internet. Message content may be reviewed to ensure compliance with this policy. As a user of the email system, you are required to:

1. Register any important email information within Council's records management system.

2. Ensure emails are accurate and of a suitable quality. This includes all information, photographs, graphics, messages, sounds or other materials provided.
3. Assume email correspondences are of good nature.

6.4.1 Prohibited Email Usage Responsibilities

Under NO circumstances should users:

1. Ask for or send offensive remarks, proposals, or material. If you receive unsolicited offensive material, you should delete it from your mailbox. Under no circumstances should offensive material be forwarded on
2. Harass other employees or external persons
3. Represent personal opinions as those of Weddin Shire Council.
4. Send or access copyrighted information in a way that violates copyright.
5. Send or forward on any email chain letters or virus hoaxes.
6. Send any information that contravenes Council's Cyber Security Policy and other policies relevant to the User.
7. Use Council email for personal purposes such as signing up for social media or subscribing to non-work related items.
8. Use personal email for Council-related purposes, such as sending or receiving Council-related communications, accessing Council data, or conducting official Council business.

6.5 Obtaining IT Support

IT support should be sought in house; either in person, via telephone (found in the Telephone Directory) or via email (found in the Global Address Book). Under no circumstances should staff attempt to resolve IT issues for themselves or for another employee unless qualified to do so. Unauthorised attempts to address technical problems may lead to further complications, data loss, or potential security breaches.

6.6 Hardware Upgrades

Hardware is monitored by the Corporate Services Department to ensure optimal performance and functionality. Hardware is attempted to be replaced when devices have reached their useful life. By maintaining up-to-date hardware, Council ensures that its employees can efficiently run software applications necessary for conducting council business.

6.7 Acceptable Use of Work Mobile Phone

Council may provide staff with mobile phones to be used exclusively for Council-related tasks, including access to Council email. All provided mobile phones must be protected with a screen lock to uphold data security and prevent unauthorised access in case of loss or theft. Adherence to this policy is essential for maintaining Council data confidentiality and ensuring responsible mobile phone usage for Council business.

6.8 Non-Compliance

Users who are suspected of violating any of their responsibilities as listed in these policies may be investigated and subjected to disciplinary action. Such disciplinary action may include (but is not limited to):

1. Verbal and written warnings.
2. Suspension of network privileges including email and/or Internet privileges.
3. Termination of employment for Council employees or contracts for consultants or contractors.
4. Code of Conduct complaint, review and investigation.
5. Referral of the issue to an external agency, for example Office of Local Government, Worksafe NSW and Fair Work Commission.

7 DEFINITIONS

Key Terms	Meaning
Council	Weddin Shire Council
Devices	Any computing device including Desktops, Laptops, Tablets and Phones.
ICT	Information and Communication Technology
Information Services	The interconnected set of components used to collect, store, process and transmit data and digital information
Peripheral	A component that can be added to a device in order to increase its capabilities. Peripherals include keyboards, mice, printers, scanners, external hard drives, webcams, monitors, speakers, and USB flash drives.
Pirated Software	Unauthorised copies or illegal distribution of copyrighted software without the permission of the software's copyright owner.
Screen Lock	Security feature found on various electronic devices to prevent unauthorised access. Normally in the form of a swipe pattern or PIN.
Users	Council employees, Councillors, consultants, contractors, volunteers, and work placement students.

Title: Draft Information Services Usage		
Department: Corporate Services		
Version	**Date**	**Author**
1.15.1	20 August 2009	Council
1.15.2	21 March 2013	Council
1.15.3	16 March 2017	Council
1.15.4	17 August 2023	DRAFT, Josh Dawes
1.15.04	16 November 2023	Adopted Resolution 258/23
This policy may be amended or revoked at any time and must be reviewed at least three (3) years since its adoption (or latest amendment). The Director of Corporate Services will be responsible for the review of this policy. Review of this policy will incorporate relevant legislation, documentation released from relevant state agencies and best practice guideline. **Review Date: 16 November 2026**		
Amendments in the release		
Amendment History	**Date**	**Detail**
Annexure Attached:		
Noreen Vu **General Manager**		