POLICY:-	
Policy Title:	Information Technology Security, Cyber and Acceptable Use Policy
File Reference:	F21/29
Date Policy was adopted by Council initially:	20 June 2024
Resolution Number:	89/24
Other Review Dates:	N/A
Resolution Number:	N/A
Current Policy adopted by Council:	20 June 2024
Resolution Number:	89/24
Next Policy Review Date:	2027

PROCEDURES/GUIDELINES:-	
Date procedure/guideline was developed:	N/A
Procedure/guideline reference number:	N/A

RESPONSIBILITY:-	
Policy developed by:	Director of Environment and Planning and Manager IT
Committee/s (if any) consulted in the development of this Policy:	N/A
Responsibility for implementation:	Chief Executive Officer
Responsibility for review of Policy:	Director of Environment and Planning

1. Scope

This Information Technology Policy applies to Councillors, contractors and all employees of Upper Lachlan Shire Council (ULSC) who use information and communication technologies for or on behalf ULSC.

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

2. Objective

Upper Lachlan Shire Council is committed to building a high quality Information Security Management System.

This is achieved by:

(a) Managing access to Council information and customer information based on business need and sensitively of information.
(b) Implementing a set of controls to manage the implementation of security in line with this policy.
(c) Periodically reviewing risks and the effectiveness of controls intended to manage those risks.

3. Policies Statement

3.1 Access Control

Users are provided access to information, applications and systems based on their business requirement and role within the organisation. Access to any Council related information will require authentication into the system to prove their validity.

Authentication methods can vary depending on the sensitivity of the data being accessed or the location it is accessed from.

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 or Chief Executive Officer.

Any changes to the access of data a user requires will need to be approved by their Director or the Chief Executive Officer. All requests of this nature will need to be made through the IT Helpdesk, accompanied by an approved Change Request form.

3.2 Endpoint Protection

Endpoint protection methods are utilised on Council systems as a means of maintaining system integrity and keeping devices as safe as possible.

Quarantining of potentially harmful links/attachments/files is in effect as well as file and vulnerability monitoring.

All staff within the organisation have a responsibility to make safe choices regarding their use of the systems – This includes but it is not limited to:-

- external links,
- attachments,
- files,
- login pages or external devices e.g. USB sticks.

Users must not click/open links or attachments from unknown, suspicious or untrustworthy sources. Any suspicious links or files must be reported to the IT Helpdesk immediately.

3.3 Communications

Email / Teams / Social Media – Public related comms, separate from internal comms. Communications systems supplied by Council are provided to facilitate business activities. These types of systems may include but are not limited to: Email, Instant Messaging, Telecommunication and Social Media.

The use of these systems and the content within, remains the ownership of Council. Usage and activity over these systems are logged and monitored by Council.

The usage of Council's communication systems is to be used in an effective, safe, ethical and lawful manner.

Users are permitted to use Council's computer network for limited and reasonable personal use. However any such personal use must not impact upon the user's work performance or Council resources or violate this policy or any other Council policy.

Any misuse of these systems will be reported and handled in conjunction the Council's Code of Conduct.

3.4 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 leaving their computer unsecured may be subject to retaking educational courses or in severe cases 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.

3.5 Mobile Devices

Where required, users may be issued with a mobile device to perform tasks related to their role. This may include mobile phones, tablets, GPS trackers or Toughbooks.

Devices issued are provided to facilitate business activities and are owned by Council throughout its lifecycle, including all data inherent within the device.

Devices issued to staff will be centrally managed by the IT department to maintain sufficient policies, patching and available applications.

Security policies will be applied to every device requiring each be protected by PINs/Passwords as a minimum. Council retains the right to conduct inspections of any mobile device that it owns or manages without prior notice to the user or custodian. The device must be returned to the IT department upon request as soon as practically possible.

Devices supplied by Council must not be altered in any way. This may include but is not limited to:

- unauthorised upgrades,
- addition of components,
- removal of components (including transferring a Council SIM card to a personal phone),
- altering configuration or security settings,
- installation of non-approved applications, and
- jailbreaking a device.

Services related to mobile devices (e.g. Telephone Numbers or Data SIMs or similar) are owned by Council at all times and any usage of a personal nature shall not adversely impact Council operations or impose costs onto Council.

Users of these services are not to engage in activities that could cause additional financial charges to Council. Such activities may include but are not limited to: long distance calls, subscription services, reverse back calls, 1900 area code calls.

Any device issued to a member of staff is not to be reissued or borrowed by anyone else within or outside of the organisation without prior approval from a director or the Chief Executive Officer.

Any device changing ownership/custodianship should be returned to the IT department to be wiped / reconfigured before being reissued.

3.6 BYOD – Bring your own device

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

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.

3.7 Computer Systems and Equipment.

The computer systems and equipment are to be used for business purposes in the course of normal day to day operations. Personal use must be reasonable, appropriate and not impact on a Council Official's productivity, system performance or bring Council into disrepute.

Users must not connect personally owned computing devices, computer peripherals, USB devices, digital cameras, etc to computer systems or networks owned or managed by Council. If users do bring personal equipment to work, this is at their own risk and Council is not responsible for the device or anything stored on it.

Users provided a computing device acknowledge that the device and the information stored on it is the property of Council. All devices and peripherals provided, should be returned to the IT department when a user ceases employment at Council.

The equipment or device and the information stored on it can be inspected to confirm compliance with security and acceptable use requirements or used in any manner, and at any time, by authorised Council Officials or their agents. Council is not responsible for any personal information that may be stored on the device. Data may be removed from Council systems as a result of inspection or automation if they are defined as not work related.

Computer equipment supplied by Council must not be altered or added to in any way. This would include but is not limited to:

- unauthorised upgrades

- addition of components
- removal of components
- altering configuration or security settings
- installation of non-approved applications

Any changes required to devices need to be requested to the IT helpdesk and subsequently approved by a Department Director or the Chief Executive Officer.

Any changes made to the configuration or maintenance of the device must be done by Council's IT department or their designated agent.

Computers or equipment provided to an employee of Council are for the sole use of that individual unless stated otherwise at the point of issue or by exception from the Chief Executive Officer – Users must not lend or make accessible any device or equipment that has been allocated to them by Council for business activities to anyone external to Council.

All provided computers will be imaged to contain Council's approved applications. Users are not to attempt to remove any software/applications or install anything on the device. Any changes required to the device are to be made by the IT business unit in conjunction with a Helpdesk request and subsequent approval from a director or the Chief Executive Officer.

3.8 Cyber Crime and Security Incidents

A cyber incident is an occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it.

Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information or networks to be compromised in any way is considered serious misconduct, including:

i. security breaches or disruptions of network communications. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes;
ii. port scanning or security scanning. These activities are expressly prohibited unless sanctioned by the Manager IT & GIS for the purposes of testing network security;
iii. executing any form of network monitoring which will intercept data not intended for Council official's host, unless this activity is a part of Council official's normal duties or has been duly authorised;
iv. circumventing user authentication or security of any host, network or account or running password cracking programs;
v. interfering with, or denying service to any user other than Council official host (for example, denial of service attack);

vi. using any program, script, command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally;
vii. downloading, installing or executing any file containing malware which may damage or compromise computer systems or data;
viii. copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use;
ix. creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with Council's or another organisation's email service;
x. downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by Council or not;
xi. providing or selling Council's information without approval and for personal gain; and
xii. defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using Council's resources that would bring Council into disrepute.

Upon discovery of a potential security incident, staff should notify the IT helpdesk as soon as possible to coincide with Council's Data Breach Policy.

Penetration Testing

Council will conduct penetration testing on at least annually or when there are major changes to Council's information systems.

3.9 Data Management

Data and information created, modified, saved, transmitted or archived using Council systems remains the property of Council.

All Council information and data must be stored in approved Council information repositories. This includes EDRMS, Council applications and other approved shared repositories.

Data should not be stored on portable devices without being backed up on Council servers in the first instance.

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.

All uses of data, including replication, deletion and retention must comply with the *NSW State Records Act 1998.*

3.10 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/ Department 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. Review of the site will be conducted by the IT department and access will be permitted pending approval by the Manager IT/GIS.

3.11 Legal Compliance

Users must not disclose any confidential information belonging to Council or otherwise coming into their possession during the course of their employment, except as expressly permitted under any of Council's policies or as required by law.

Users may be required to sign a confidentiality or non-disclosure agreement. Information may be classified as follows:

- not to be stored information which may not be captured or saved in electronic systems;
- confidential information restricted to a small number of people;
- internal use only information which may be known by Council Officials, but not by anyone external to Council; and
- public information that is approved for public dissemination.

All intellectual property (including patents, copyrights, trademarks, inventions, designs or other intellectual property) created and/or developed by Council Officials while at work or while using Council's equipment is the exclusive property of Council.

Information held in all computer systems and networks owned or managed by Council is subject to the provisions of privacy legislation (including but not limited to GIPA and State Records Act) and users should be aware of their obligations in respect of managing and using the information and providing information to third parties.

3.12 Password and Authentication

Passwords are an employee's electronic authorisation used to gain access to Councils IT systems. Employees are responsible for the security of their accounts and their passwords.

Usernames and passwords must not be shared with anyone inside or outside of the organisation. It is important that each individual accessing Council systems use their own login to access resources.

Shared or generic user accounts are prohibited unless express permission is given from the Chief Executive Officer. A record of these accounts need to be kept for auditing purposes.

Password and authentication requirements will be set based on the most current best practice industry standards. Information regarding this can be found on the ULSC Intranet.

Passwords are not to be written down, saved in electronic folders or similar or be available for others to see. Temporary passwords must be sent in a secure manner. Users should never access systems under another individual users login.

Password managers and 2 Factor Authentication (2FA) are an important use in securing accounts and access. Where possible, Password Managers and 2FA will be a required use on Council related accounts – especially from externally accessible areas.

3.13 Patch Management

All devices provided by Council will be subject to regular patching and updates to keep systems compliant and in-line with industry standard best practices.

Patching schedules will be defined by the IT department as part of a regular maintenance schedule, in addition to any out-of-band updates coming from critical vulnerabilities that may arise.

3.14 Printing

Printers are made available for staff to use within the organisation for business purposes.

As Council strides towards being a sustainable entity and help to reduce against waste; it is highly encouraged to consider whether a document needs to be printed or should it be issued as a digital copy.

Usage of colour print vs black and white should be limited and completed only when essential.

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.

Under no circumstances should a Council employee attach an unknown USB storage device to Council IT Systems for the purpose of printing.

3.15 Remote Access

Remote access to Council's systems enables users to access data stored on Council's systems from a location outside of the Council buildings. This is enabled through the use of a Virtual Private Network (VPN).

Remote users are only permitted to access systems and data they have been approved to access for the purposes of fulfilling their work obligations to Council. All other access is considered unauthorised.

Access will only be granted once the following documents have been completed and approved:

Upper Lachlan Shire Council Employees:

- The Information Technology Security, Cyber and Acceptable Use Policy being signed;
- ULSC Remote Access Request Form is completed; and
- ULSC Change Request Form is completed and approved by a Director or the Chief Executive Officer.

3rd Party Outside of ULSC:

- Application for Remote Access is completed; and
- Remote Access Agreement is completed and approved by the Manager IT/GIS.

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

Accessing Council's IT systems remotely is not permitted by personal computers or similar, remote access is only permitted through Council issued IT hardware.

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.

4. Responsibilities

- *Elected Council*

  Approve and adopt this Policy for official use by Council.

- *Chief Executive Officer and Department Directors (MANEX)*
  To support implementation of this policy and enforce the policies terms and conditions and advise IT when management and access action is required.

- *Council employees, Councillors and contractors*
  Ensuring the engagement of information technology service providers and vendors is via the IT team, to allow repeatable and consistent vendor management practices.

  Ensuring IT are aware of all software purchases, enabling effective IT service budget management, IT environment management (no duplicated services) and IT security.

  Protect IT assets from damage and misuse. Information and Network Access may be revoked at any time by the Chief Executive Officer if there is a reasonable suspicion that the continued provision of access to information assets and systems is not in the overall interests of ULSC and to prevent unauthorised disclosure, modification, removal and destruction of information or IT assets.

5. Other Relevant Legislative Provisions and Related Policies

- Local Government Act 1993;
- State Records Act 1998;
- Electronic Transaction Act 1999;
- Privacy and Personal Information Protection Act 1998;
- Independent Commission against Corruption Act 1988;
- Government Information (Public Access) Act 2009;
- Code of Conduct;
- Data Breach Policy;
- Information Technology (IT) Strategic Plan;
- Digital Information Security Policy;
- Internet and Email Policy;
- iPad Policy;
- Mobile Phone Policy;
- GIPA Policy;
- Privacy Information Management Plan;
- Records Management Policy;
- Business Continuity Plan;
- Fraud and Corruption Prevention Policy.

6. Variation to Policy

That Council reserves the right to vary the terms and conditions of this policy.