ADOPTED	
COUNCIL MEETING MIN	**66/25**
DATE:	19 MARCH 2025

VERSION NO	**1.0**
REVIEW DATE	MARCH 2028
FILE NUMBER	**INT800022**

Objective

This Policy sets out the standards of acceptable use and behaviour expected of Users operating Mid-Western Regional Council's ("Council") electronic telecommunications facilities and equipment.

Scope

This policy applies to Mid-Western Regional Council employees, Councillors, contractors, consultants, members of the public, and other users (jointly referred to as "Users"). It also applies to the use of information, electronic and computing devices, and network resources to conduct Council business or interact with internal networks and business systems, whether owned or leased by Mid-Western Regional Council, the employee, or a third party.

The usage stated above is applicable when a User is at any workplace of the Council or other place where work for the Council is carried out, whether the User is performing work at the time or not.

The policy also sets out the type of monitoring that will be carried out in Council's workplace relating to the use of Council's Computer Network by all Users.

Related policies and plans

- Code of Conduct
- Electronic Telecommunications Acceptable Use – Acknowledgement Form
- Workplace Bullying Policy
- Anti-Discrimination Policy and EEO Policy
- Social Media Policy
- State Records Act 1998 and Regulation 2010
- Workplace Environment Statement – Core Values
- Workplace Surveillance Act 2005
- Records Management Policy
- IT Strategic Plan 2024/28

Definitions and Terms

'**Computer Network' or 'Electronic Telecommunications Systems'** – includes all Council's internet, email, hand held device and computer facilities which are used by Users, inside and outside working hours, in the workplace of Council (or related corporation of Council) or at any other place while performing work for Council (or related corporation of Council). It includes, but is not limited to, desktop computers, laptop computers, mobile phones including smart phones, tablet devices, PDA's, other means of accessing Council's email, internet and computer facilities, (including, but not limited to, a personal home computer which has access to Council's IT systems).

'**Computer Surveillance'** – Surveillance by means of software or other equipment that monitors or records information input or output, or other use, of Councils Computer Network (including, but not limited to, the sending and receipt of emails, text messages and the accessing of websites).

'**Intellectual Property'** – all forms of throughout the world, including copyright, patent, design, trademark, trade names and all Confidential Information and know-how and trade secrets.

'Mobile Device Management (MDM)' – Software that is installed on all Council issued electronic devices. MDMs are the administrative area dealing with deploying, securing, monitoring, integrating, and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimise the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network.

Policy

1. Personal Use

1.1. Employees will ensure that the use of Council's Computer network is related to the conduct of Council operations

1.2. Personal use of Council's Computer Network should be kept to a minimum (e.g., not operating a personal/private business)

1.3. Council provided accounts are not to be used to sign up for personal services or subscriptions (e.g., streaming services and social media)

1.4. Personal use should not impact on any work-related priorities or violate this policy or any other Council policy or procedure.

1.5. While Council respects the right of Users to privacy, Council gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed or saved by any User while using Council's electronic telecommunications facilities or equipment for the User's personal purposes.

1.6. Users should be aware that copies of personal files may be made during Council's usual network backup processes.

1.7. User's personal files may be reviewed during Council's usual network administration processes.

1.8. Random samples of files are taken to ensure that breaches of this procedure or any law are not occurring.

1.9. Council is not responsible for the loss of any personal data that is stored on the Council's computer network.

1.10. Employees provided with a Council mobile phone also have the benefit of using the mobile phone for their personal use. Employees must use the services provided responsibly; repetitive excess usage can be investigated.

1.11. Council will not under any circumstances permit the use of Council equipment for prohibited purposes and will take immediate action against any User found to be engaging in any prohibited activities.

2. Software

2.1. Users must not modify or disable Council information assets and digital services, and system settings provided for malware protection, software updates, or scans unless the activity is authorised by a relevant IT staff member.

2.2. Users must not make deliberate attempts to disrupt computer system performance, nor harm or destroy hardware or data in any form on Councils Computer Network.

2.3. Users must only use computer software or versions of software that have been authorised and tested for use on Council's Computer Network.

2.4. Users must never knowingly import or download unlicenced or unauthorised software on Council's Computer Network.

2.5. Users must not gain unauthorised access (hacking) into any other computer either internal or external to Council or attempt to deprive other Users of access to or use of Council's Computer Network.

3. Access Controls

3.1. Users must be authorised to access Council's network.

3.2. Users must only access, use or share Council information to the extent that it is authorised to fulfill the assigned job duties.

3.3. Users must keep passwords confidential, and change them when prompted, or as required.

3.4. Users must only use their own username/login and/or password when accessing the computer network. Account passwords that are assigned to a single user must not be revealed to others.

3.5. Users must not log into Council's Computer Network on behalf of any other user.

3.6. Users in possession of Council issued electronic devices must always handle the device in a responsible manner and ensure that the device is kept safe and secure.

3.7. Users have a responsibility to promptly report the theft, loss or unauthorised access of Council devices or data to their manager or supervisor.

3.8. Users are required to lock or shut down their device when it is not in use or unattended.

3.9. All Council owned mobile communication devices (tablets, phones) are required to have Mobile Device Management software to ensure complete device security and be secured with a 6-digit pin at a minimum.

4. Emails and Communications

4.1. If a User receives any communication of which the content is in breach of this policy, regardless of whether it includes text, images, materials or software, the Information Technology (IT) team should be contacted immediately. The User must not forward the email or text message to any other person unless expressly asked to do so by the IT Manager or delegated officer.

4.2. Users must promptly exit an inappropriate website should a user inadvertently access such a site.

4.3. Users must not intentionally send (or cause to be sent), upload, download, use, retrieve, or access any email or text message or material using Council's computer network that:

- Is obscene, offensive, or inappropriate. This includes text, images, sound or any other material sent either in an email or in an attachment to an email, or through a link to a site (URL) or in a text message or as an attachment to a text message. For example, material of a sexual nature, indecent or pornographic material.
- Causes (or could cause) insult, offence, intimidation, or humiliation.
- May be defamatory or could adversely impact the image or reputation of Council. A defamatory message or material is such that it is insulting or lowers the reputation of a person or group of people.
- is illegal or unlawful.
- affects the performance of, or causes damage to Council's systems in any way, including computer and network systems; or
- Gives the impression of or represents, gives opinions, or makes statements on behalf of Council without the express authority of Council.
- Send or cause to be sent chain or SPAM emails or text messages in any format.
- Introduce malicious programs into the network or server (viruses, trojans, etc.)

4.4. Users are prohibited from using third-party email systems and cloud storage servers to conduct Council business, to create or memorialise any binding transactions, or to store or retain email on behalf of Council. Approval to utilise these solutions is from the Manager, IT, or delegated officer.

4.5. Users must not use Council's electronic telecommunications facilities and/or equipment for personal gain or commercial activities not directly related to Council.

4.6. Users are prohibited from automatically forwarding Council emails to a third-party email system (as above). Individual messages which are forwarded by the user must not contain Council confidential or above information.

4.7. Cyber-bullying with not be tolerated and will be treated in the same manner and in accordance with Council policies.

5. Education and Training

5.1. Users must undertake appropriate cyber security awareness education and training as per the Council's training program.

6. Content

6.1. Users must not use Council's computer network to:

- Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using Council's computing facilities, except as permitted by law or by contract with the owner of the copyright.
- To create any legal or contractual obligations on behalf of Council unless expressly authorised by Council.
- Disclose any confidential information of Council or any customer, rate payer, client or supplier of the Council unless expressly authorised by Council.

7. High Risk Roles

7.1. High Risk Roles possess privileged access to Councils critical platforms. To safeguard identified High Risk Roles and their attributed privileges, additional requirements are required by staff in these roles.

7.2. High-Risk Role users will receive additional training specific to their elevated privileges

and responsibilities, which will be completed by all staff in these roles annually.

7.3. High Risk roles are defined as:

- Executive staff
- Assistants to Executive staff
- Systems Administrators
- Users with access to privileged systems
- User with privileged access to systems.

8. Surveillance and Monitoring

8.1. Users should be aware that although access controls and security features of Council's electronic telecommunications facilities and equipment give the User the illusion of privacy, their browsing activities, email, text message and file content can still be scrutinised. Access controls are put in place to prevent unauthorised access not to guarantee privacy.

8.2. The ICT team are authorised to access an area, files, and electronic communications on the network, even those that are password protected. This authority extends to local resources including hard drives and removable media.

8.3. All files, data and electronic communications that are stored on the network are routinely subject to backup. Backups of data are retained in accordance with legislative requirements. Backups may be accessed at any time for the purposes of file retrieval and for monitoring use of Council's electronic telecommunication devices and systems.

8.4. Council by default blocks access to certain sites and content. Users who require access to blocked websites should contact the ICT team in the first instance and may require the approval of their manager.

8.5. Files or data that are inappropriate or non-work related may be deleted without notice.

8.6. Filtering devices to detect and block inappropriate electronic communications or which deny access to websites or other content which is inappropriate may be deployed and monitored.

8.7. Unauthorised use that breaches this policy may lead to measures as outlined throughout this policy.

8.8. Council reserves the right to prevent or cause to be prevented the delivery of an email or text message sent to or from a User, or access to an internet website by a User, if the content or the email or text message or the internet website falls under the Prohibited Conduct listed above.

8.9. Council reserves the right to scrutinise and determine the suitability of any information distributed through electronic telecommunications devices using any Council resources.

8.10. On a continuous and ongoing basis during the life of this policy, Council may carry out electronic monitoring and surveillance of any User at such times of Council's choosing and without further notice to any User.

9. Record Keeping

9.1. All Users are responsible for ensuring their electronic communications (inwards, outwards, and internally) and all other electronic records are recorded on the relevant Council file in line with document management procedures. This includes emails, text messages, photographic messages, and voice messages.

10. Non-Compliance

10.1. Any use of Council's electronic telecommunications facilities and equipment thought to be inconsistent with this procedure may be monitored and investigated. As part of the investigation process, the Users' rights to access any or all the facilities and equipment may be revoked.

10.2. If inappropriate or prohibited use occurs, disciplinary action may be taken including issuing a warning, suspension, demotion, or termination of employment; or, for Users other than employees, the termination or non-renewal of contractual arrangements.

10.3. Users other than employees will be managed on a case-by-case basis. In addition, Council may refer the matter to appropriate authorities for prosecution under the relevant criminal codes.

11. Responsibilities and Obligations

11.1. All individuals who access Council's electronic telecommunications facilities or equipment are personally responsible for:

- Ensuring they understand and comply with this policy,
- Completing any required training to maintain competency, and
- Signing the Electronic Telecommunications – Acceptable Use Acknowledgement Form before utilising Council systems or equipment for communication.

11.2. Supervisors and Managers are responsible for making users aware of this policy and facilitating training where appropriate. However, users remain responsible for ensuring they understand and adhere to the policy.