Communication Devices, Internet and Intranet Policy
(Revision 1)

	Name	Position	Signature	Date
Responsible Officer	Sue Mitchell	Manager Corporate and Community Services		9 December 2022
Authorised By	John Scarce	General Manager		9 December 2022

Document Revision History	
Previous Policy 1	Communication Devices Policy
Date adopted by Council:	27 July, 2017
Minute Number:	150/07/17
Previous Policy 2	Internet, Intranet, Email and Computer Use Management Policy
Date adopted by Council:	24 April, 2018
Minute Number:	81/04/18
Revision Number:	1
Policies Incorporated and Renamed:	**Communication Devices, Internet and Intranet Policy**
Review Date:	November/December 2022
Date adopted by Council:	9 December 2022
Minute Number:	202/12/22
Next Review:	See item 19 of this Policy
Revision Number:	
Review Date:	
Date adopted by Council:	
Minute Number:	

December 2022

Contents

1. Purpose 3
2. Scope 3
3. Requirements for Use 3
4. Remote Access 4
5. Personal Use 4
6. Inappropriate Use and Prohibited Conduct 5
7. User Access 6
8. Blocking Email or Internet Access 6
9. Use of Email 7
10. Email - Leave Arrangements 8
11. Email - Prevention of Virus Attacks 8
12. Email Disclaimer 8
13. Password Policy 9
14. Multi-Factor Authentication 9
15. Cyber Security Breach 10
16. Monitoring Use and Breaches of this Policy 10
    Type of Surveillance in the Workplace 10
    What will the Surveillance Records be used for 10
17. Staff Acknowledgement 11
18. Related Council Policies 11
19. Policy Review 11

Attachment 1 12

1. Purpose

The purpose of this policy is to document Council's requirements and expectations regarding the use of its communications devices. The policy aims to ensure Councillors and Council employees understand the way in which Council's communication devices should be used in the organisation. Council makes its communication systems available to employees to enable efficient sharing and exchange of information in the pursuit of Council's goals and objectives.

It also sets out the types of surveillance that will be carried out relating to the use of Council's computer network and systems.

2. Scope

This policy applies to all Councillors, Council employees, contractors, consultants, temporary and casual employees and any other authorised personnel offered access to Murrumbidgee Council communication devices and systems. Communication devices and systems include, but are not limited to:

- All computers (laptop and desktop)
- All iPads, tablets, data phones
- Council's email system
- All telephones (land-line and mobile)
- All copying devices
- All two-way radios
- Facsimile machines

It also applies to using these devices to access the intranet or internet.

3. Requirements for Use

Users must comply with the following rules when using Council's computer networks:

- Users must use their unique username/login code and password when accessing the computer network;
- Users should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is to do so for legitimate business reasons;
- Users in possession of Council's electronic equipment must, at all times, handle the equipment in a responsible manner to ensure the equipment is kept secure;
- Users should ensure that, when not in use, or unattended, the computer device is locked or shut down;
- A disclaimer is automatically included in all Council's emails and must not be removed;
- If a user receives an email to which the user suspects contains a virus, the user should not open the email or attachment to the email and should immediately contact the Manager Corporate and Community Services or Council's ICT service providers;

- If a user receives an email in which the content, including an image, text material or software is in breach of this policy, the user should immediately delete the email and report the matter to the Manager Corporate and Community Services. The user must not further distribute the email; and
- All information created should be registered into Council's records management system in accordance with the Records Management Policy.

4. Remote Access

Council provides remote access to contractors and selected staff to facilitate flexible working arrangements and employees' productivity. There are two access methods available:

- *RDPlus*, which is a secure connection using a web browser to gain remote control of a dedicated computer within the office. This may be used by employees on their home computer, controlling the work computer.
- *OpenVPN*, which provides a secure tunnel from the persons' computer back to the office network, and is typically used by employees with laptops, or contractors.

5. Personal Use

Reasonable personal use of Council's communication devices is permissible; however, personal use is a privilege, which needs to be balanced in terms of operational needs; its use must be appropriate, lawful, efficient, proper and ethical. Council recognises that:

- Employees are also private citizens with individual personal needs and obligations
- Employees may need to make use of communication devices for personal purposes
- There is a reasonable limit to which employer communication devices may be used for personal purposes

Every employee has a responsibility to be productive and act appropriately during their work time, therefore, personal use:

- Should be infrequent and brief
- Must not disrupt Council communication systems
- Should not interfere with the employee's job responsibilities or detrimentally affect the job responsibilities of other employees
- Employees reasonably suspected of abusing personal use requirements will be asked to explain such use
- Councillors and staff who have been allocated communications devices are responsible for all access to websites, emails, downloads etc that occur on that device whilst at work, at home or elsewhere by themselves or by any other person

6. Inappropriate Use and Prohibited Conduct

The use of Council's communications devices to make or send fraudulent, offensive, sexually explicit, unlawful or abusive information, calls or messages is strictly prohibited.

Any employee identified as the initiator of fraudulent, unlawful or abusive calls or messages will be subject to disciplinary action and possible criminal prosecution.

Staff who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to their Manager/Supervisor.

All employees should be aware that it is illegal to record telephone conversations unless authorised under relevant legislation to do so.

Users must not send, upload, download, use, retrieve or access any email or material on Council's computer network that:

- Is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent in an email or an email attachment through a (URL) link to a site, or in a text message or a text message attachment. This includes material of a sexual nature, indecent or pornographic material;
- May be defamatory or could adversely impact the image or reputation of Council eg a defamatory message or material that is insulting or lowers the reputation of a person or a group of people;
- Is illegal, unlawful or inappropriate;
- Affects the performance of, or causes damage to, Council's computer system in any way; or
- Gives the impression of, or is representing, giving opinions or making statements on Council's behalf with the express authority of Council. Users must also not transmit or send Council documents or emails or text messages (in any format), to any external parties or organisation unless expressly authorised to do so.

Users must not use Council's computer network for the following:

- To knowingly 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 computer facilities except as permitted by law or by the owners or the copyright;
- In a manner contrary to Council's Code of Conduct;
- To create any legal or contractual obligations on behalf of Council unless expressly authorised by Council;
- To disclose any confidential information of Council or any customer, rate payer, client or supplier of the Council, unless expressly authorised by Council;

- To install software or run unknown or unapproved programs on the computer network. Under no circumstances should users modify the software or hardware environments on the computer network unless authorised by the Manager Corporate and Community Services to do so;
- To gain unauthorised access (hacking) into any other computer within Council or outside Council, or attempt to deprive other users access or use of Council's computer network;
- To send or cause to be sent, chain or SPAM emails or text message in any format;
- To use Council computer facilities for personal gain, for example running a personal business; and
- Any form of harassment via the computer network

Users must not log into another user's computer network facilities without the correct authorisation

7. User Access

Council will provide access based on the following principles:

- Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.
- Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

8. Blocking Email or Internet Access

All staff access to the internet is routed through Council's firewall.

Council reserves the right to prevent (or cause to be prevented), the delivery of an email to or from a user, or access to a website (including social media), by a user, if the content or the email or website is not consistent with the policy or is considered:

- Obscene, offensive or inappropriate. This includes text, images, sound or other material sent either in an email message or in an attachment to a message or through a link to an internet website (URL) or in or attached to a text message;
- Will, or may, cause insult, offence, intimidation or humiliation;
- Defamatory or may incur liability, or adversely impacts on the image or reputation of the Council. A defamatory message or a message or material that is insulting or lowers the reputation of a person or a group of people;
- Illegal, unlawful or inappropriate;
- To have the potential, or affect the performance of, or cause damage to, or overloads Council's computer network, or internal or external communication in any way; and
- To give the impression of, or is representing, giving opinions or making statements on behalf of the Council without the express authority of Council.

Blocked sites that are required for business activities should be approved by a member of the executive team prior to being unblocked.

In the case that an email is prevented from being delivered to or from a user, the user will receive a prevented delivery notice. The notice will not be given if:

- The email was considered to be spam or contained potentially malicious software or;
- The content of the email (or any attachment) would, or might have, resulted in an unauthorised interference with, damage to, or operation of, any program run or data stored on any of Council's equipment; or
- The email (or any attachment) would be regarded by any reasonable person as being, in all circumstances, menacing, harassing or offensive.

Council is not required to give a prevented delivery notice of any email message sent by a user if the Council is not aware (and could not reasonable be expected to be aware), of the identity of the user who sent the email, or is not aware that the email was sent by the user.

9. Use of Email

Email (external/internal) forms part of the official business communications of Murrumbidgee Council (see Council's Records Management Policy).

As such, email is governed by the same legislative requirements (State Records Act 1998, Government Information (Public Access) Act 2009, Privacy & Personal Information Protection Act 1998,) as all other Council records.

All email is accessible through Council's email server. All business related emails must be registered in the electronic document management system and not stored in email accounts.

All emails, both external and internal, are archived by Council and are available for review. Such reviews will be authorised by the relevant manager or a member of senior management.

In addition to inappropriate usage restrictions for communication devices, email is <u>not</u> to be used for:

- Sending or distributing 'chain' letters, 'hoax' mail or for other mischievous purposes (SPAM).
- Unauthorised accessing of data or attempt to breach any security measures on the system, attempting to intercept any data transmissions without authorisation.
- Sending email messages of a defamatory nature. Email can be used as evidence in a court of law, Council and the sender can both be held liable for publishing defamatory material.

10. Email - Leave Arrangements

When employees are on leave, the 'Out of Office Assistant' is to be used to inform each sender:

- When the employee will be back from leave, and that
- Urgent matters should be emailed to Council's central email address: mail@murrumbidgee.nsw.gov.au

To use the 'Out of Office Assistant' simply do the following in Microsoft Outlook:

Click on 'File'
Click on 'Automatic Replies (Out of Office)'
Click on 'Send automatic replies" (include leave start and end dates)
Type in your message (for inside and outside my organisation)
Click on 'OK'

When the employee returns to work they are to ensure that the 'Out of Office Assistant' is turned off and all relevant matters have been, or will be dealt with.

11. Email - Prevention of Virus Attacks

Recipients of email messages that have a suspicious title are NOT to open the email message without prior consultation with the Manager Corporate and Community Services. Although virus protection software is installed, there is no guarantee that this will prevent all viruses from infiltrating the Council network.

Where documents are received as an attachment to an email message, these attachments, under all circumstances, must be scanned by anti-virus software to avoid the potential risk of infecting the Council network.

Software programs received as an attachment to an email message are not to be installed onto a PC or Council's network under any circumstances without the prior permission of the Manager Corporate and Community Services.

12. Email Disclaimer

The following should be included as a standard footer, on every external email sent from Council's system:

PLEASE NOTE: Unless stated otherwise, this email, together with any attachments, is intended for the named recipient(s) only and may contain privileged and confidential information. If received in error, you are asked to inform the sender as quickly as possible and delete this email and any copies of this from your computer system. If you are not the intended recipient of this email, you must not copy, distribute or take any action that relies on it and any form of disclosure, modification, distribution and/or publication of this email is prohibited. We have taken precautions to minimise the risk of transmitting software viruses, but you are advised to carry out your own virus checks on any part of this message including any attachments. We cannot accept liability for

any loss or damage caused by software viruses. The views expressed in this email are not necessarily those of the Murrumbidgee Council unless stated otherwise.

13. Password Policy

Council's password policy is managed and enforced by Veritech, Council's external ICT provider.

These include minimum length, age and complexity requirements and limitations on password re-use.

All staff are required to exercise caution when using passwords on cloud (or web) based services.

In addition to the internal password policies, the following rules are to be followed:

- Use different passwords on each cloud system accessed. This reduces the impact of a compromised system.
- Do not keep passwords written in unsecured locations. In preference to writing passwords down, use a password manager application.
- Do not sign into work services using single sign-on linked to social media accounts (e.g., Facebook).
- Use multi-factor authentication whenever it is available.
- Avoid websites with unsecured logins. Typically, websites should start with HTTPS:// and provide an indicator like a padlock near the address to be considered secure. If they just provide HTTP://, then don't provide any personal details or passwords.

Mobile devices don't typically have the layers of security protection of computer systems, so employees using mobile devices will need to exercise appropriate caution when accessing company or cloud resources. Any personal mobile device that contains Council information (such as emails) must have a locking function supported by PIN as a minimum, and preferably biometrics such as fingerprint or face recognition.

14. Multi-Factor Authentication

Multi-factor Authentication (MFA) or Two Factor Authentication is a security technique that requires a person to have something they know (usually a password or PIN) and something they have (generally a Time-based One Time Passcode (TOTP) or a security certificate).

Council's systems will require the use of MFA when connecting remotely.

When connecting to any third-party system, it is advisable that MFA is used to protect logins. When systems process sensitive information, MFA must be used.

15. Cyber Security Breach

If any person suspects a breach of security, they are to notify the Cyber Security Manager (the Chief Financial Officer) and Veritech (02 6964 5377) as a high priority incident.

Any suspected breach may result in a reportable event which will involve further investigations. Therefore, it is necessary that accurate records are kept. These records could include a timeline of events, decisions log, and relevant systems information, including screenshots.

16. Monitoring Use and Breaches of this Policy

Council may monitor, copy, access and disclose any information or files that are stored, processed or transmitted using Council's equipment and services. Such monitoring will be used for legitimate purposes only (such as legal discovery) and in accordance with any relevant privacy legislation and/or guidelines.

Reviews of email and phone usage may occur at the request of the relevant Director or Council's General Manager.

Individuals who breach this policy may be subject to disciplinary action pursuant to Council's Codes of Conduct and the NSW Local Government (State) Award, if applicable. Such disciplinary action may include termination of employment.

Type of Surveillance in the Workplace

Throughout the period of application of this policy, Council will carry out activity surveillance of any user at such times of Council's choosing and without further notice to any user.

Surveillance occurs in relation to:

- Storage volumes;
- Internet sites including time of access, duration of access and content downloaded;
- Downloaded volumes;
- Suspected malicious codes or viruses;
- Emails;
- Computer hard drives; and
- Mobile device content including, but not limited to, text message and records.

Council retains logs, backups and archives of computer activities which may be subject to audit. Such records are the property of Council, and Council is obligated to abide by State and Federal laws, and these records may be used in evidence to legal proceeding under those laws or within internal investigations into misconduct.

What will the Surveillance Records be used for

Council may use and disclose the surveillance records under the following circumstances:

- For the purpose related to the employment of any employee, the retention of any other user or related to Council business activities;
- Use or disclosure to a law environment agency in connection with an offence;
- Use or disclosure in connection with a legal proceeding;
- Use or disclosure where Council reasonably believes it to be necessary to avert an imminent threat of serious violence or to the injury to any person or substantial damage to property;
- Use or disclosure can occur under circumstances of assault, suspected assault, suspected harassment, stalking or bullying, theft or suspected theft of, or damage to, Council's property, including information, equipment or facilities;
- Councillors' surveillance records will be used when requested by regulatory bodies such as the Independent Commission Against Corruption.

17. Staff Acknowledgement

The People and Culture Officer must ensure that all new, and existing, staff receive a copy of this policy. The People and Culture Officer must ensure that staff sign the Murrumbidgee Council Communications Agreement (Attachment 1) after the staff member has read the policy document.

18. Related Council Policies

- Murrumbidgee Council Records Management Policy.
- Murrumbidgee Council Codes of Conduct.

19. Policy Review

This Policy:

- To be reviewed within the first year of the new Council term;
- May be reviewed and amended at any time at Council's discretion (or if legislative or State Government policy changes occur).

Attachment 1

COMMUNICATION DEVICES, INTERNET AND INTRANET AGREEMENT

NAME: _____

DEPARTMENT: _____

- I understand my responsibility as a user of Murrumbidgee Council's communication devices and systems.
- I have received, read, understand and will abide by the Murrumbidgee Council Communication Devices, Internet and Intranet Policy.
- I understand that any breach of the Communication Devices, Internet and Intranet Policy may result in disciplinary action under Council's Code of Conduct and may be dealt with pursuant to the NSW Local Government (State) Award.
- I also understand that if I commit any breach of this policy, my access privileges may be revoked.

User Signature: _____ Date: _____