# Internet, Intranet, Email and Computer Use Management Policy

| | Name | Position | Signature | Date |
|---|---|---|---|---|
| Responsible Officer | **Alison Coe** | **Assistant General Manager-Corporate & Community Services** | | |
| Authorised By | **Craig Moffitt** | **General Manager** | | |
| Date Adopted by Council: | | **24 April 2018** | | |
| Minute No: | | **81/04/18** | | |

## Revision History

| Version | Date | Prepared/Amended | Approved By | Revision Date |
|---|---|---|---|---|
| V1 | | Assistant GM, Corporate & Community Services | Council | April 2018 |
| V2 | | | Council | December 2019 |
| V3 | | | Council | December 2020 |
| V4 | | | Council | |
| V5 | | | Council | |
| V6 | | | Council | |
| V7 | | | Council | |
| V8 | | | Council | |
| V9 | | | Council | |
| V10 | | | Council | |

## Change History

| Version | Change Details |
|---|---|
| V1 | Initial policy |
| V2 | Annual Review of Policy |
| V3 | |
| V4 | |
| V5 | |
| V6 | |
| V7 | |

## Related Documents

| Document Title |
|---|
| Local Government Act 1993 |
| Local Government (General) Regulation 2005 |
| Government Information (Public Access) Regulation 2009 |
| Murrumbidgee Records Management Policy |
| Murrumbidgee Council Code of Conduct |
| Murrumbidgee Council Mobile Devices Policy (TBC) |
| Workplace Surveillance Act 2005 |

# Table of Contents

## Purpose and Objectives

This policy sets out:

1. The standards of behaviour expected of persons using Murrumbidgee Council's computer facilities while conducting Council business; and
2. The type of surveillance that will be carried out relating to the use of Council's Computer network and systems.

## Authority

This policy has been authorised by the General Manager. Ownership of this policy rests with the Assistant General Manager of Corporate and Community Services.

## Application

All Councillors, staff, contractors and consultants ("users"), utilising Council's computer facilities must comply with this policy, the attached user agreement and associated policies when conducting official business for Council.

## User of the Internet, email and Computers

Where use is allowed, users are entitled to use Council's Computer Network only for legitimate business purposes.

Users are permitted to use Council's Computer Network for limited and reasonable personal use within personal work time, such as designated breaks or outside core working hours. However, any such personal use must not impact upon the user work performance, Council resources, create a cost to Council or violate this policy or any other Council policy.

## Requirements for Use

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

1. Users must use their unique username/login code and password when accessing the computer network;
2. 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;
3. Users in possession of Council's electronic equipment, must at all times, handle the equipment in a responsible manner to ensure the the equipment is kept secure;
4. Users should ensure that when not in use, or unattended, the computer device Is locked or shut down;

5. A disclaimer is automatically included in all Council's emails and must not be removed;
6. 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 Assistant General Manger Corporate and Community Services or Council's ICT service providers
7. If a user receives an email in which the content, include 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 Assistant General Manager, Corporate and Community Services. The user must not further distribute the email; and
8. All information created should be registered into Council's records management system in accordance with the Records Management Policy.

## Prohibited Conduct

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

    a. Is obscene, offensive or inappropriate. This include 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 test message attachment. This includes material of a sexual nature, indecent or pornographic material;
    b. May be defamatory or could adversely impact the image or reputation of Council. A defamatory message or material that is insulting or lowers the reputation of a person or a group of people;
    c. Is illegal, unlawful or inappropriate;
    d. Affects the performance of, or causes damage to Council's computer system in any way; or
    e. Gives the impression of, or is representing, giving opinions or making statements on Council' 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.

2. Users must not use Councils Computer Network for the following:

    a. To knowingly violate copyright o other intellectual property rights. Computer software that is protected by copyright is not to be copied from or into or by suing Council's computer facilities except as permitted by law or by the owners or the copyright;
    b. In a manner contrary to Council's Code of Conduct;
    c. To create any legal or contractual obligations on behalf of council unless expressed authorised by Council;
    d. To disclose any confidential information of Council's or any customer, rate payer, client or supplier of the Councils unless expressly authorise by Council;

e. 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 Assistant General Manager, Corporate and Community Services to do so;
f. To gain unauthorised access (hacking) into any other computer within Council or outside Council, or attempt to depries other user or access or use Councils computer network;
g. To send or cause to be sent, chain or SPAM emails or text message in any format;
h. To use Council computer facilities for personal gain, for example, running a personal business; and
i. Any form of harassment via the computer network

3. User must not log into another user's computer network facilities without the correct authorisation

## Blocking Email or Internet Access

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;

a) 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 (UIRL) or in or attached to a text message;
b) Cause or may cause insult, offence, intimidation or humiliation;
c) 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;
d) Illegal unlawful or inappropriate;
e) 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 a way; and
f) To give the impression of or is representing, giving opinions or making statements on behalf of the Council without the express authority of Council.

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:

a) The email was considered to be SPAM or contained potentially malicious software or;
b) 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
c) The email (or any attachment) would be regarded by any reasonable person as being in all the 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 mail or is not aware that the mail was sent by the user.

## 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:

a) Storage volumes;
b) Internet sites including time of access, duration of access and content downloaded;
c) Downloaded volumes;
d) Suspected malicious does or viruses;
e) Emails;
f) Computer hard drives; and
g) 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 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:

a) For the purpose related to the employment of any employee, the retention of any other user or related to Council business activities; or
b) Use or disclosure to a law environment agency in connection with an offence; or
c) Use or disclosure in connection with a legal proceeding;
d) Use or disclosure where Council reasonably believes to be necessary to avert an imminent threat of serious violence or to the injury to any person or substantial damage to property;
e) 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;
f) Councillors surveillance records will be used when requested by regulatory bodies as the Independent Commission Against Corruption.

## Enforcement

Users must comply with the policy requirements. Any breach of this policy may result in disciplinary action including employment termination.

Other disciplinary action that may be taken includes, but is not limited to, issuing a warning letter, suspension or disconnection of access to all or part of, Council's computer network whether permanently or on a temporary basis.

## Definitions

| | |
|---|---|
| **Confidential information** | Includes, but is not limited to, all Council's non-public information about the organisation and affairs of the Council such as: pricing information (internal costs and pricing rates), software, procurement , marketing or strategic plans, exclusive supply agreement or arrangements; commercial and business plans; contractual agreements with third parties. |
| **Computer Surveillance** | Means surveillance by means of software or other equipment that monitors or records information input or output, or other use, of Council's Computer Network including, but not limited to, the sending and receipt of emails and accessing of websites. |
| **Computer Network** | Includes all Council's internet, email and computer facilities which are used by the defined users, inside and outside of Council working hours, within the Council workplace or at any other place while performing work for Council. This includes, but is not limited, desktop computers, mobile devices including a personal home computer which has access to Council's systems. |
| **Intellectual Property** | Means all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name and all confidential information. |

| | |
|---|---|
| **Mobile Devices** | Includes, but is not limited to, laptop computers, personal digital assistant, tablet (including IPads) smart phone or any other handheld electronic devices or similar product. |
| **Social Networking** | Includes but is not limited to sites such as Facebook, Twitter, Instagram, YouTube, blogs etc. |