Use of Information Technology and Communication Devices Policy

Policy Approval and Distribution

Approved by	Council Resolution
Responsible Officer	IT Officer, Peter McCallum
Council Service Unit	Information Technology
Next Review Date	01 June 2022

Version Control

Ref	Date	Description	Council Resolution
0.1	26-06-2018	Presented to Council for adoption	124/2018

Purpose

The objective of this policy is to provide clear guidelines for staff and Councillors in their use of computers, internet, email, telephone and other electronic media and devices in the conduct of Council-related activities.

This policy seeks to:

- Preserve the integrity and efficiency of information technology and communication equipment by providing guidelines to clarify what constitutes appropriate conduct and use of the equipment;
- Ensure the use of information technology and communication equipment complies with the organisation's obligations to maintain a workplace that is efficient, harmonious and without risk of discrimination or harassment resulting from improper use; and
- Outline the ramifications of failing to abide by the guidelines contained in this policy.

Scope

This policy applies to:

- All Council staff, including employees, casuals, consultants and contractors
- Councillors

Compliance with this policy is a condition of each staff member's employment with Council. A breach of any part of this policy may, depending on the circumstances, be regarded as a serious breach of the staff member's employment contract with Council.

A failure to comply with this policy and any relevant directions given by management may result in the following action being taken against a staff member or Councillor:

- Counselling (including intensive training on this policy and the appropriate use of facilities)
- Disciplinary action regarding "inappropriate use" of the facilities, including cancellation of access to any or all of the facilities
- Dismissal of staff where access and/or the distribution of material outlined in this policy are unacceptable.

Definitions

Information technology and communication equipment means and includes any electronic equipment or computer software provided to Councillors or staff for use in the performance of their duties, either in general or specific terms including, but not limited to: computers, including desktop computers, laptops/notebooks, tablets and handheld devices; printers; scanners; digital cameras or any other digital imaging equipment; all software and programs provided to facilitate work needs; network operating systems (eg Windows); all network infrastructure including data cabling and transmission equipment; all forms of email; internet access; and mobile phones which may or may not be connected to the internet and/or email.

Legislative Framework

The guidelines in this policy are based upon the requirements of legislation and other related policies, so as to protect Council, staff and Councillors from legal action.

Relevant legislation is as follows:

- NSW Anti-Discrimination Act 1977
- NSW Privacy and Personal Information Protection Act 1998
- NSW State Records Act 1998
- Evidence Act 1995
- Federal Sex Discrimination Act 1984
- Federal Racial Discrimination Act 1975
- Federal Crimes Act 1900
- Federal Copyright Act 1968
- Federal Defamation Act 1974
- Defamation Act 2005 (NSW)
- Employees Liability Act 1991 (NSW)
- Crimes Act 1914 (Commonwealth)
- Federal Disability Discrimination Act 1992
- Telecommunications Act 1997

Related CGRC Policies

Relevant CGRC policies are as follows:

- Code of Conduct
- Payment of Expenses and Provision of Facilities for Mayor and Councillors
- Records Management Policy
- WH&S Policy
- Staff Training Policy – under development
- Social Media Policy – under development

Review Period

This document is to be reviewed every two (2) years to ensure that it remains relevant and meets legislative requirements.

Policy Statement

Council recognises that access to information technology and communication devices is required as a convenient and effective means of communication, both internally between staff and departments, and externally with other councils, groups or individuals.

Council's position is that information technology and communication devices are necessary to conduct business activities, however recognises the need to comply with the organisation's obligations in maintaining a workplace that is efficient, harmonious and without risk of discrimination or harassment resulting from improper use of the information technology and communication equipment supplied.

Policy Provisions

1. System Security

It is the responsibility of the Information Technology service unit to provide, maintain and monitor the necessary hardware and software to minimise security risks posed to internal information technology and communication networks. Virus protection is based at the server level and filters all threats at this layer in the network.

It is the responsibility of each staff member and Councillor to maintain the confidentiality and security of their own password. Councillors and staff should ensure that they:

- Log off the network or password lock their workstation whenever leaving it unattended for long periods of time, including attending meetings and lunch breaks.
- Do not attempt to gain access to another staff member's or Councillor's log-in ID or password.
- Do not disclose passwords to any persons other than those within the Information Technology service unit for system-related requirements.
- Create complex and unique passwords. It is recommended that passwords are a minimum of 8 characters incorporating upper and lower case letters, special characters and at least one number.

2. Network access

The IT Officer must be informed when a new employee or Councillor require access to Council's network. The IT Officer will consult with the new employee's supervisor to determine appropriate levels of system access and security privileges. The IT Officer is responsible for the procurement of any new information technology or communication equipment required.

Councillors and staff must not grant access to Council's network to persons outside of the organisation unless approval is obtained from the General Manager. This includes work experience students, volunteers, external contractors, etc. Where approval is conditionally given, such persons are not permitted to use an existing user's log-in ID or password. In such circumstances, the IT Officer will arrange a temporary account with the appropriate levels of system access and security privileges.

To help avoid the spread of viruses, Councillors and staff must not bypass Council's network security by accessing the internet directly by personal modems, personal access points, switches or routers or other unauthorised means, unless permission has been granted by the IT Officer.

Councillors and staff must not attempt to access, copy, damage, delete, insert or alter any information held on Council's computer equipment or network beyond the privileges granted by the IT Officer for the performance of their normal work duties.

Councillors and staff must remain cautious when accessing any file or data from an external source. If Councillors or staff suspect a file or data from an external source may pose a risk to Council's network, the file or data must be brought to the IT Officer's attention who will scan the file and determine its risk to the Council network. If any staff or Councillor suspects that a virus has been introduced into Council they must notify the IT Officer immediately.

Councillors and staff must not attempt to install or remove software or hardware into Council's network without prior approval and direction from the IT Officer.

On termination of employment or otherwise at the request of the General Manager, the IT Officer will ensure access to Council's network is deactivated. The IT Officer will ensure all information technology and communication equipment issued has been returned, unless alternate arrangements have been agreed to by the General Manager.

3. Handling and usage of equipment issued

Staff must use and care for the information technology and communication equipment in their possession in a responsible manner. Breakages, damage or loss of equipment must be reported by staff to their immediate supervisor and/or the IT Officer. Information technology and communication devices are not to be left in vehicles while unattended. Information technology and communication equipment is issued for work purposes, not for 'family' use, and are therefore not to be used by children for games or other applications under any circumstances.

In instances of misuse or neglect, breakages, damage or loss of equipment may lead to the need for reimbursement to the Council of any associated costs incurred by Council in relation to the repair or replacement of the affected equipment.

Staff are required to keep information technology and communication equipment clean, and in serviceable condition to the best of their ability.

4. Usage provisions

Council accepts that its information technology and communication equipment may on occasion be used for personal reasons. Acceptable personal use includes access during lunch breaks or outside normal work hours and consistent with all other sections of this policy. However, Councillors and staff must remember that the primary purpose of Council's information technology and communication equipment are tools for conducting business and to enhance the overall effectiveness of the organisation. The provision and maintenance of computer equipment and consumables is a cost to Council's business activities and therefore excessive personal use of these facilities can undermine the effectiveness of the organisation. Excessive personal use may lead to disciplinary action and/or privileges removed.

Council will monitor network access logs and internet and telephone (including mobile phone) usage patterns and investigate any significant variances. Charges incurred by Council for excessive calls, data and/or internet use may need to be reimbursed to Council by the user. Should a staff member either exceed their prepaid allocation or receive a monthly statement that is 'out of the ordinary', the staff member may be required to justify the increase in use to their supervisor. In the event that the misuse of network access, telephone or internet connections are found, the staff member will be responsible for the payment of the charges deemed excess by the relevant supervisor and may face disciplinary action and/or privileges removed.

Use of Council's computer equipment, email and internet may be granted to an individual Councillor or staff for work-related study purposes by agreement with their supervisor.

Councillors and staff must not use Council's computer equipment to maintain or support a personal business activity under any circumstances.

Staff must avoid any action or situation that could create the appearance that Council property is being improperly used for a staff member's benefit or the benefit of any other person or third party.

5. Copyright

All Councillors and staff must respect the copyright and any other intellectual property rights of third parties. Copyright protects the exclusive right of the copyright holder to copy, publish, perform, broadcast and sell copyrighted material. Councillors and staff must not download material from the internet or otherwise receive and use information that is owned by a third party unless they have the written permission of that party. Examples of possible breaches of copyright can include forwarding emails or copying or downloading copyright material (including computer programs, screensavers, sounds and images) that have copyright protection.

As a general rule, under copyright law downloading from the internet for personal research is allowed. However, downloading material for distribution to others or for business purposes will require the permission of the third-party owner.

6. Storage of Data

All Council data will be permanently stored on Council's servers for backup and security purposes. Disk space on individual Council desktop computers, tablets or laptops should only be used as temporary storage, or for transitional purposes only.

Staff are responsible for ensuring business communications are registered in Council's document management system. Refer to Council's Records Management Policy for further guidance on the requirements of record keeping.

7. Email usage

Council accepts that email may on occasion be used for personal use reasons. Acceptable personal use includes sending short personal emails during lunch breaks or outside normal work hours. However, Councillors and staff must remember that the primary purpose of email is to enhance business activities and the overall effectiveness of the organisation.

Councillors and staff must not use email (including personal email) to:

- Conduct illegal activities
- Send email messages that in any way could, or would be likely to, bring Council's name into disrepute
- Send email messages (with or without attachments) which contain inappropriate or offensive material of a sexual, racial, defamatory, abusive, obscene or discriminatory nature
- Distribute "junk mail" or electronic chain letters including emails seeking donations and those providing pyramid selling schemes or advertising
- Send unauthorised emails from another person's email address or impersonating another person
- Send emails which are likely to be perceived as harassment, intimidation or an unwanted invasion of privacy
- Send non-urgent emails (e.g. jokes) to large numbers of people (whether within Council or not)
- Send personal email to any person who does not wish to receive it. If a recipient asks a user to stop sending him or her email, their request must be observed.

All emails sent or received from Council's system remain the property of Council. For legal purposes, emails are a formal document and have the same standing in court as paper documents.

Councillors and staff should not expect that email is confidential or private. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

Council has implemented a maximum size for allowable email messages and also restricts email messages that contain certain attachments or content which have been known to contain viruses from either entering or leaving Council. The IT Officer should be contacted on a case by case basis if these limitations are found to be too restrictive. Staff should note that council has these limitations in place to protect our network and infrastructure. The IT Officer will regularly review the logs of blocked or quarantined emails and will release those that do not pose a risk to Council's network and which appear to be business related. If staff are aware of a missed or undelivered email the IT Officer should be notified. The email scanner and email software will be accessed to investigate any emails and causes for undeliverable emails.

Whilst Council does not wish to become a censor, to ensure that the guidelines contained in this policy are followed, Council retains the right to access or view users' email sent via the corporate network. Council will only access information created or stored on Council's email system under the direction of the General Manager for disciplinary procedures or where there is a valid business requirement. Justification for access must be provided, logged and recorded to provide evidence of the decision made to access a staff member's email account. Councillors and staff must not access, or attempt to access, another staff members' or Councillor's email account.

If a staff member or Councillor receives offensive email from outside Council, they should immediately delete it. In the event that further material is received, the staff member should advise their supervisor. A Councillor should advise the General Manager.

7.1 Management of Email Messages

Email is a valid form of communication within Council. Councillors and staff must manage their email mailbox personally by ensuring that emails received are actioned within acceptable times, unwanted emails are cleared, and business communications are registered in Council's document management system. Refer to Council's Records Management Policy for further guidance on the requirements of record keeping.

7.2 Out of Office Notifications

Staff are responsible for setting up an Out of Office notification to notify senders of periods of absence. Out of Office replies should include duration of absence and an alternate staff member who may be contacted for business purposes in your absence.

7.3 Standards for Outbound Email

The IT Officer is responsible for the creation and maintenance of all email signatures. Staff must not edit their own email signatures. The format of email signatures is as follows:

Joe Bloggs
Important Officer
Cootamundra-Gundagai Regional Council

COOTAMUNDRA-GUNDAGAI REGIONAL COUNCIL

P: 1300 459 689

M:

E: joe.bloggs@cgrc.nsw.gov.au

W: www.cgrc.nsw.gov.au

8. Internet Usage

The policy provisions regarding internet usage apply to any device which may access online sites or services, including desktop computers, laptops, tablets and mobile phones.

Council accepts that internet facilities may on occasion be used for personal use reasons. Acceptable personal use includes browsing the internet during lunch breaks or outside normal work hours. However, Councillors and staff must remember that the primary purpose of the internet facilities is to enhance business activities and the overall effectiveness of the organisation.

Councillors and staff must not use the internet facilities to:

- Intentionally access sites which contain pornography, or inappropriate or offensive material of a sexual, racial or discriminatory nature
- Solicit, download, store, or distribute pornography, inappropriate or offensive material of sexual, racial or discriminatory nature
- Access internet chat clients or internet relay chat networks
- Conduct gambling or gaming activities
- Conduct private transactions of a personal gain/profit nature, either directly or indirectly
- Stream music or programs.

Councillors and staff should be aware that internet sites accessed by them can record Council's name, IP address and passwords. Council can monitor sites that Councillors and staff are accessing and Council reserves the right to do so to ensure that the guidelines contained in this policy are followed. Council reserves the right to block access to sites which it deems to be inappropriate.

The internet is not a secure method of sending information. Therefore, when sending confidential information (for example business information, client details, pricing, or any personal or private information about individuals), careful consideration should be given as to whether alternative means of communication are preferable.

Council recognises that social media provides new opportunities for dynamic and interactive two-way communication which can complement existing communication and further improve information, access and delivery of key services. Refer to Council's Social Media policy for further guidance on the acceptable business and personal use of social media.

9. Telephone Usage

The policy provisions regarding telephone usage apply to any telephony device, including mobile phones and desk handsets. The use of mobile phones or desk handsets by Council staff is permitted and encouraged where such use is suitable for business purposes and supports the goals and objectives of Council. Mobile phones may be issued to staff to assist in the conduct of their normal work duties with Council. Mobile phones often have internet and email capabilities and the rules associated with email and internet use also applies to mobile phones.

The use of mobile phones whilst driving is forbidden unless the hands free function is activated. It is an offence to use mobile phones whilst operating a motor vehicle and the incursion of expiations and fines will be solely at the staff or Councillor's cost. Any vehicle damage incurred as a result of this practice which is not recoverable through insurance, may be recovered from the staff member.

9.1 Installation of Applications

It is possible to install Applications (or "Apps") on a work mobile phone. Staff are reminded that it is a work mobile phone and applications should be work-related. Staff must seek approval for the installation of applications where the application is not free. The IT Officer must be notified and approve the installation of any application to ensure there is no conflict or network breach.

The installation and purchase of applications for personal use must be kept to a minimum. Any costs incurred by Council for downloading, accessing or using the application (including data charges) may be recoverable by Council from the end user.

9.2 Message bank

Message bank is installed on all mobile phones within our network and is to be used and accessed. It is a requirement for all staff who have been issued a Council mobile phone to record a voice message for the purposes of the message bank. This voice message is to include a welcome greeting, and the name and/or role of the staff member.

10. Work Health and Safety

It is the responsibility of Council to ensure Councillors and staff are aware of any relevant issues pertaining to the correct handling and usage of information technology and communication hardware and software.

It is the responsibility of the IT Officer that all equipment meets the current Australian safety standards. All equipment (including mobile phones, desk handsets, cables, computers, printers, tablets and other related electronic equipment) must not be purchased without the authorisation of the IT Officer to ensure compliance with work health and safety, our network specifications and requirements. The IT Officer is responsible for the demonstration of the correct usage and handling of information technology and communication equipment.

Refer to Council's WH&S Policy for further guidance on the requirements of work-related health and safety practices.

11. Education and Training

The IT Officer is responsible for ensuring all system users are made aware of this policy. New employees will be given a copy of this policy as part of induction processes.

The Information Technology service unit is responsible for ensuring all staff and Councillors have access to training materials to assist in the provisions of this policy.