

INFORMATION TECHNOLOGY & COMMUNICATIONS

Objective

To set out the general principles associated with the use of Council's Information Technology resources including acceptable and unacceptable use.

Scope

This policy applies to all elected members and employees in their use of Council's information technology and communications and all associated equipment, services and contracts. The General Manager and Senior Management Team are responsible for the implementation and monitoring of Council's Information Technology and Communications policy and associated processes however, responsibilities may be delegated to specific employees or external agencies as identified.

Policy

Information Technology (IT) facilities are provided to assist elected members and employees to conduct normal Council business.

All users must accept full responsibility for using the IT facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people. Use must be in accordance with Council's procedures and all relevant Federal and State legislation.

Mobile devices issued by Council are to be used for work related purposes. Mobile devices are issued to the position and not the person. If the person is on leave or otherwise absent from work, the mobile phone is to be passed on to the person acting in the position if required. Mobile devices issued to positions that require email to be sent to the device are equipped with a data package considered appropriate for the expected usage.

Any abuse of Council's mobile device usage will lead to the phone being confiscated and/or disciplinary action being taken in accordance with the Local Government (State) Award 2014 provisions.

Council reserves the right to recover excess call and data usage charges incurred by the elected member or employee responsible for the mobile device, where it is deemed not business related.

Council reserves the right to recover from an elected member or employee responsible for the mobile device, the cost to replace a mobile device to the equivalent of the original if it is deemed the device was deliberately damaged or device replacement is more frequent than would normally be expected.

An elected member or employee must report immediately any loss, theft or damage to any equipment issued to them.



Acceptable Use

The following use is accepted and encouraged:

- Usage that supports Council's strategic planning including its vision, values and Code of Conduct
- Usage that relates to the provision of services to the residents, ratepayers, general community and other employees
- Using the infrastructure to complete duties relevant to the employee's position within Council.

Personal Use

Elected members and employees are permitted incidental use to information technology and communications equipment and services for private purposes where such use is open, accountable and transparent. Private use must always be acceptable and lawful and not interfere with elected member's or employee's capacity or ability to perform their respective duties.

Information technology and communication services and associated equipment is primarily for Council's business use and must be in accordance with legislative requirements and the guidelines set out in this policy.

Council may negotiate with elected members and employees for additional costs or expenses associated with approved use, where requested.

Misuse can damage Council's corporate and business image, infringe copyright and intellectual property generally, and could result in litigation being brought against both Council and the user.

Passwords and Password Confidentiality

Passwords are an elected member's/employee's electronic authorisation on Council's information technology system. Individuals are responsible for the security and regular changing of their password(s). Elected members and employees are required to take reasonable precautions to ensure their password is not known by any other party unless written approval is provided by the elected member/employee granting access. No password shall be provided to anybody that is not an elected member or employee of Council.

You may be required to disclose your password(s) to the General Manager on request.

Users must be aware that access passwords and other protection methods are in place, however there is a general level of "insecurity" for communications via the Internet and associated sites and email.

It is prohibited for anyone to:

- Hack into other systems
- Read or attempt to determine other people's passwords
- Breach computer or network security measures, or
- Monitor electronic files or communications of others without their written permission.

Logging Off

Network users are required to log off at the end of the business day. Failure to do so may result in unauthorised personnel accessing confidential data. The onus is on the user to log off. Users are also encouraged to "Lock" their screens when away from their terminal for short periods of time. Users will be shown how to lock their computers during their induction.

Out of office Assistant (Microsoft Outlook)

Users are required to use this function in Microsoft Outlook (email client) when they know that they will be out of the office for more than 1 business day.

Identity

No email or other electronic communication may be sent which conceals or attempts to conceal the identity of the sender.

The only exception is where system functionality is intended to keep the identity of the sender anonymous, such as feedback forums or electronic surveys.

Confidential Messages

Elected members and employees must exercise care and discretion with electronic communications such as tenders, contracts, confidential agenda's, minutes and reports.

Email messages are perceived to be instant in nature and instantly disposed of. There is a backup facility that retains a copy of the file even if it is eliminated from the senders and recipients computer.

Improper statements can give rise to liability – personally and for Council. Elected members and employees must work on the assumption that messages may be sent, forwarded, transmitted or printed by someone other than the intended recipient.

Controlled or limited distribution of messages must not be assumed.

Accordingly, elected members and employees must be cautious about committing totally private, sensitive or confidential messages and related documents to electronic communication.

Elected members and employees must be aware that email messages, even if expressed to be confidential, may be disclosed in Court proceedings, Freedom of Information requests, investigations by the Ombudsman, competition authorities and regulatory bodies. It may be necessary for Council under Court or regulatory body appointments to retrieve and / or disclose electronic information and communications.

Elected members and employees are provided access to records held by Council in the performance of their duties.

Software

Downloading and / or installing unlicensed / illegal software is prohibited. Users must liaise with Council's IT department prior to purchasing any software.

Virus protection

Viruses are most prevalent in non-work related emails. The majority of viruses are enclosed in chain letters and joke attachments to emails. Non text files or unknown messages must not be opened / forwarded and should be made known to Council's IT staff.

Users are not permitted to interfere with the operation of virus protection software on Council computers and computer based systems.

Email Signature

Users who have an email address are required to use the approved format/font email footer as provided at setup. Users are required to use this footer, which contains a disclaimer, for all emails sent from their Council email address:

This message is intended for the addressee named and may contain confidential information. If you are not the intended recipient, please delete it and notify the sender. Views expressed in this message are those of the individual sender, and are not necessarily the views of the [Gilgandra Shire Council](#) unless otherwise stated. For the purposes of the Copyright Act, the permission of the holder of copyright in this communication may be taken to have been granted, unless stated otherwise, for the copying or forwarding of this message, as long as both the content of this communication and the purposes for which it is copied or forwarded are work-related.

Users are not permitted to change this footer, without prior consent from the IT Department.

Unacceptable and Unlawful Activities

Elected members and employees are not to access or send material that is prohibited or potentially prohibited, provocative, pornographic, offensive, abusive, sexist or racist. This includes not forwarding to others any material of this nature that is received and includes, but not limited to social media sites such as Facebook, MySpace and Twitter.

Allowing unauthorised persons to use Council's information technology infrastructure (eg friends, customers and family) is also unacceptable.

Unlawful activities are absolutely prohibited, including:

- Gaining access to and downloading any material which is prohibited or potentially prohibited, pornographic, offensive or objectionable
- Engaging in any conduct which breaches any laws and regulations
- Accessing, viewing or downloading any material containing and/or promoting embarrassment, bullying, harassing, defamatory, abusive, sexist, racist, threats of violence or otherwise illegal material against another person, including elected members and employees
- Breach of Council's Code of Conduct or Values

- Access for the purposes of personal financial gain, where that access is in breach of Council's *Public Interest Disclosures - Reporting Policy*
- Disperse corporate data to Council's customers or clients without prior authorisation
- Accessing internet gambling sites
- Contain personal opinions about statements or conduct of other elected members and employees that may be defamatory or derogatory
- Violation of copyright legislation
- Circumventing, filtering, intentionally downloading software or other content access device or software; and
- Interfering with electronic records management information.

There are serious repercussions arising from such transmission including criminal offences and offences under the Broadcasting Services Amendment (Online Services) Act 1999 (Commonwealth).

Notice of Workplace Surveillance

Workplace Surveillance Act 2005 – Section 10. Notice of surveillance required.

1. Surveillance of an employee must not commence without prior notice in writing to the employee.

Note: Subsection (6) provides for an exception to the notice requirement.
2. The notice must be given at least 14 days before the surveillance commences. An employee may agree to a lesser period of notice.
3. If surveillance of employees at work for an employer has already commenced when an employee is first employed, or is due to commence less than 14 days after an employee is first employed, the notice to that employee must be given before the employee starts work.
4. The notice must indicate:
 - a) the kind of surveillance to be carried out (camera, computer or tracking), and
 - b) how the surveillance will be carried out, and
 - c) when the surveillance will start, and
 - d) whether the surveillance will be continuous or intermittent, and
 - e) whether the surveillance will be for a specified limited period or ongoing.
5. Notice by email constitutes notice in writing for the purposes of this section.
6. Notice to an employee is not required under this section in the case of camera surveillance at a workplace of the employer that is not a usual workplace of the employee.

Workplace Surveillance Act 2005 – Section 17. Restrictions on blocking emails or Internet access

1. An employer must not prevent, or cause to be prevented, delivery of an email sent to or by, or access to an Internet website by, an employee of the employer unless:
 - a) the employer is acting in accordance with a policy on email and Internet access that has been notified in advance to the employee in such a way that it is reasonable to assume that the employee is aware of and understands the policy, and
 - b) in addition, in the case of the preventing of delivery of an email, the employee is given notice (a "prevented delivery notice") as soon as practicable by the employer, by email or otherwise, that delivery of the email has been prevented, unless this section provides that a prevented delivery notice is not required.
Maximum penalty: 50 penalty units.
2. An employee is not required to be given a prevented delivery notice for an email if delivery of the email was prevented in the belief that, or by the operation of a program intended to prevent the delivery of an email on the basis that:
 - a) the email was a commercial electronic message within the meaning of the [Spam Act 2003](#) of the Commonwealth, or
 - b) the content of the email or any attachment to the email would or might have resulted in an unauthorised interference with, damage to or operation of a computer or computer network operated by the employer or of any program run by or data stored on such a computer or computer network, or
 - c) the email or any attachment to the email would be regarded by reasonable persons as being, in all the circumstances, menacing, harassing or offensive.
3. An employee is not required to be given a prevented delivery notice for an email sent by the employee if the employer was not aware (and could not reasonably be expected to be aware) of the identity of the employee who sent the email or that the email was sent by an employee.
4. An employer's policy on email and Internet access cannot provide for preventing delivery of an email or access to a website merely because:
 - a) the email was sent by or on behalf of an industrial organisation of employees or an officer of such an organisation, or
 - b) the website or email contains information relating to industrial matters (within the meaning of the [Industrial Relations Act 1996](#)).

In accordance with the Workplace Surveillance Act 2005 Section 10 and Section 17, surveillance is carried out as follows:

How the surveillance will be carried out

Council uses appropriate software to monitor the use of email and internet access. Such software quarantines, deletes and forwards email as the software determines the status of the respective email. Our internet software allows monitoring of the sites accessed, length of time spent, size of data downloaded, date and time of access and various other information regarding the sites accessed.

When an employee attempts to access a site that has been blocked, an error message will be displayed. This message will advise that access to the site has been denied because of its content.

Directors and/or Managers can request, on an ad-hoc basis, reports that detail the sites browsed, amount of time spent browsing and the amount of information downloaded/ browsed for a specified time period to ensure that Council's Internet service is not being abused.

The surveillance will be of a continuous nature.

Defamation

For the purpose of defamation law, "publication" is very broad and includes any means whatsoever that we use to communicate with each other, including Internet and email. A statement made electronically is, by its very distribution, published. A statement is also published if it is simply received electronically and forwarded electronically. Council is at risk of litigation for any defamatory material stored, reproduced or transmitted via any of our facilities. Likewise, an individual may also be open to litigation.

Copyright

Elected members and employees are required to adhere to the requirements of copyright legislation. Intellectual property rights apply to most material on the Internet, including text, graphics and sound. Elected members and employees must not assume they can reproduce, print, transmit or download material to which they have access. Usage of any material should comply with copyright legislation, as any material reproduced outside permitted uses or without the permission of the owner may result in litigation against Council.

Records Management

Electronic communications are considered Council correspondence in accordance with corporate standards and record management requirements, practices and procedures this applies to emails and any attachments. All business related emails, including attachments must be forwarded to Councils Records Management Officer.

Electronic correspondence, other than that which are personal or private in nature, are Council records and need to be retained for record keeping purposes. Council's electronic records management system is to be used for this purpose. A reply email, or confirmation of receipt of an email for important communications is recommended. This confirmation must then be added to Councils official records management system.

Housekeeping

It is the responsibility of each user to do his/her own housekeeping on a regular basis (i.e. delete messages/documents when no longer required). Council reserves the right to maximise the storage limit in each users inbox to ensure equitable use available for email storage and may increase depending on disk space.

Breach of conditions of this policy

In circumstances where an elected member or employee breaches this policy, Council reserves the right to restrict the use or access to the information technology and communications and associated equipment and services and to maintain that restriction at its discretion, Council may undertake other disciplinary action under its Code of Ethics. Where it is identified through any investigation that a criminal offence may have occurred Council will refer the matter to Police.

Indemnity by Council Members and Employees

The Council bears no responsibility whatsoever for any legal action threatened or commenced due to intentional conduct and activities of Council members and employees in accessing or using its information technology, communications and associated equipment and services. Council members and employees indemnify the Council against any and all damages, costs and expenses suffered by the Council arising out of any intended unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement.

Legal prosecution following a breach of these conditions may result independently from any action by Council.

Confidentiality

All written correspondence may become public record where it forms part of a report to Council. It is the responsibility of the author to notify Council in writing if they wish their correspondence to remain confidential.

All correspondence lodged with Council is subject to the Government Information (Public Access) Act 2009 and confidentiality cannot be guaranteed under the provisions of that legislation.

Definitions

Council – refers to Gilgandra Shire Council

Defamation – to publish a statement which is or is likely to cause the ordinary, reasonable member of the community to think less of the targeted person or to injure that person in their trade, credit or reputation

Email – A service that enables people to exchange documents or material (messages, photographs, video and music) in electronic form.

Elected Member – An elected member of Council

Employee – includes any person employed by Council and authorised persons providing services to, or on behalf of Council

Hack – To gain access into another’s computer system or files by illegal or unauthorised means

Information Technology Services and Equipment – Services and equipment provided to elected members and employees for their use in their respective roles, including but not limited to: personal computers, mobile devices (tablets and phones), associated software, printers, telephones, email and internet access and the information received or forwarded through use of such items.

Internet – A global research, information and communication network providing services such as access to information, file transfer and electronic mail including, but not limited to social media sites such as Facebook, Twitter and MySpace. Council’s webroot software limits the ability of users to access inappropriate sites.

Material – includes data, information, text, graphics, animation, speech, videos, photo, maps and music or other sounds, accessible electronically, including any combination or selection of any of these.

Security System – To protect the information on our network we have prescribed controls giving authorisation and access to files and directories in the network. Each individual has a series of passwords which allows them to access information and programs within their authority.

Email Signature – A signoff clause which allows you to add your own name, title and Council contact details.

Relevant Legislation

Workplace Surveillance Act 2005

Spam Act 2003

Government Information (Public Access) Act 2009

Local Government (State) Award 2017

Associated Documents

Nil

| | | | |
|-----------------------------|--|-----------------------|----------------------------------|
| Responsible Officer: | Director Corporate Services | | |
| Date Adopted: | 20/3/13 16/4/14 18/2/15 20/3/18 | Resolution No: | 74/13 95/14 15/15 48/18 |
| Version: | 4 | Review Date: | February (annually) |