

EMAIL & INTERNET POLICY

BACKGROUND

The Shire of Quairading provides its staff with access to information and communication facilities to enhance their ability to perform their work. In particular, access to email and the internet is provided to enable networking and access to worldwide information resources. With that access comes responsibility and accountability.

All users are required to comply with all legislation, regulations and policies applicable to the use of these devices. Like all Council assets and services, computers, email and the internet, should be used in an efficient, lawful and ethical manner, as per the Code of Conduct.

OBJECTIVE

To assist all users in the appropriate use of email and the internet and to ensure that the infrastructure is used efficiently, and the operation of the system and the reputation and integrity of Quairading Shire Council is not jeopardised. It is imperative for users to understand and comply with this policy to reduce and eliminate potential risks and losses for Council.

POLICY

Computer use in the workplace is now a standard practice and, in the ordinary performance of their tasks, employees are required to make use of increasingly sophisticated communication tools. The use of email facilities, Facebook and other electronic media outlets and the internet has significantly broadened employee access to alternative written communication channels in addition to information contained on the World Wide Web.

Users have a responsibility to use email and internet in a professional, ethical and lawful manner. All users are to use email and internet access as they would any other type of official Council communication tool. This implies that when email and internet facilities are used, the users must ensure that high standards of business communication ethics are adhered to. Users should therefore carefully consider the intended audience, tone, formality and format for all their communications.

Abuse of email or internet facilities for non-business related activities by employees may compromise the organisation and result in potentially enormous costs to Council. Examples of these costs would be excessive network bandwidth being utilised, lost productivity and potential exposure of the organisation to legal or other proceedings emanating from third parties as a result of inappropriate use of the facilities.

Access to the use of email and internet facilities is a privilege not a right. It can be withdrawn when the privilege is abused.

Council accepts no responsibility for any damage, direct or indirect, arising out of employee use of email or internet facilities.

PROCEDURE

Managers must ensure that all users within Council have access to and understand the content of this policy. Each user must familiarise themselves with the content of this policy and if anything is unclear, they should contact their Manager to discuss.

Access

All permanent, part time and casual employees will be permitted to use email and internet facilities owned by Council, where the use of such facilities assists them in performing their duties. Access may also be granted to those employees or external users such as consultants and contractors employed on a specific contractual arrangement who require access for matters directly concerned with the business of Council. Approval to make use of these facilities is given by the appropriate Executive Manager or CEO.

Private use

While email and internet access is provided as a business tool to users, its reasonable and incidental use for personal purposes is acceptable. Employees may use such services for personal use provided that such use:

- Is consistent with professional conduct;
- Does not interfere with the responsibilities of the person and their work performance;
- Does not place undue demand on Council's email and internet resources;
- Is not used for personal financial gain or personal commercial purposes;
- Will not provide the user with personal privacy rights, subject to any provisions to the contrary under Australian law;
- Will not be used to obtain unauthorised access to electronic data of other parties (internal or external).

Emails should not be used to communicate any personal details about the user or any other individual about which there may be any sensitivity or whereby that person's reputation may be injured.

Council permits the use of the internet for non-business related reasons, provided that it in no way interferes with the employee's day to day work performance and, where possible, should be restricted to outside of working hours. If Council is of the reasonable opinion that it is necessary to cancel or suspend the service, it reserves the right to do so.

Violation

Violation of this policy will be taken seriously and may result in the suspension or cancellation of the usage of electronic facilities and/or result in disciplinary action including possible termination of employment and civil or criminal liability depending on the circumstances.

Unacceptable use

Unacceptable use includes, but it not limited to:

- The transmission of any email that is of such a nature that would harm the reputation of Council;
- The transmission of any email which is unethical, maybe perceived to be a conflict of interest, or contains confidential Council information sent to individuals unauthorised to receive such information;
- The transmission of any email which contains an employee's personal view/opinion relating to any matter affecting Council;
- Users allowing anyone else to send email using their accounts (the exception being Managers who give express authorisation to Personal Assistants or other support staff);
- The transmission of any material that is unlawful, obscene, threatening, abusive, defamatory or hateful, encourages conduct that would constitute a criminal offence, gives rise to liability, or otherwise violate any local or national law;
- Users using email for commercial solicitation or for conducting or pursuing their own business interests or those of another organisation;
- The use of email for the mass distribution of hoaxes, chain letters, or advertisements; or sending rude, obscene or harassing messages;
- Sending or distributing viruses or other material which can damage electronic information systems, knowingly or intentionally;
- Excessive use of Facebook and other such sites during normal working hours;
- Excessive personal use of Council's email within normal working hours.

Monitoring of users

Council reserves the right to monitor, audit, access and keep records of internet usage and email communications and data sent from, received by and stored upon the computer network (including emails which may be sent to or by employees internally within Council or externally). It may also monitor employee's use to ascertain compliance with regulatory practices and procedures relevant to the organisation, to prevent/detect crime such as fraud or corruption, and to ensure that employees do not breach this policy regarding the use of email or internet.

In the event of suspected abuse of email or internet facilities, the individual concerned will be advised of the nature of the suspected misuse, and their account will be monitored. Should the misuse continue, Council reserves the right to implement the staff disciplinary procedure. However in all cases of suspected misuse or actual misuse of electronic facilities, Council may exercise its right to withdraw or suspend access to any or all electronic facilities for a specified period or indefinitely.

Email usage

Inappropriate use of the email technology will be reviewed on a case-by-case basis and may lead to disciplinary action up to and including dismissal. For external users, it may lead to cancellation of the contractual arrangement.

Spam/Hoax emails

Prior to opening of email messages, check if from a known source, particularly if there is an attachment.

If the sender is unknown or the email address looks unusual do not open the email or any attachments. Report the email to your Supervisor if available or contact Council's contracted IT support for assistance.

Incorrectly delivered email

Any message received, which is not intended for the recipient, must be immediately returned to the sender. All copies of the misdirected message should be deleted after it has been returned to the sender. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain. Employees encountering or receiving inappropriate material should immediately report it to their Manager.

Email attachments

Restrictions apply to the sending of attachments. Large attachments should be compressed where possible and users are requested to remove large attachments from their mailboxes. Large attachments relate to files that are greater than 25Mb. The unnecessary use of large "personal" distribution lists must be avoided due to their impact on the network. Software programs should never be attached to emails, as they are the intellectual property of Council, or they are the copyright property of the software distributor. Users must be aware of the risks associated with opening documents with macros, postscript files and installing programs received via email.

Internet usage

Excessive and inappropriate use of the internet is not permitted. This will be revised on a case-by-case basis and may lead to disciplinary action up to and including dismissal. For external users, it may lead to cancellation of the contractual arrangement. Employees encountering or receiving inappropriate material should immediately report it to their Manager.

Unacceptable use includes, but is not limited to the accessing, downloading, uploading, sending, distributing or displaying of unacceptable or illegal content from the internet, including but not limited to content that:

- is used in connection with infringement of another person's intellectual property rights;
- may be seen as defamatory, fraudulent, insulting, disruptive, harassing, intimidating or offensive to other employees (including material concerning sex, sexual orientation, race, colour, national origin, religion, age, disability or any other characteristic protected by law), or harmful to Council's morale;
- is used in connection with any attempt to penetrate the computer network or security of Council, or other computer systems, or to gain unauthorised access to any other person's computer or email; and
- is pornographic, profane or obscene.

- Use of the internet for personal reasons to conduct any commercial business which is not the business of Council (this excludes personal internet banking);
- Use of instant messaging such as MSN;
- Destruction of, or damage to, equipment, software or data belonging to Council or other clients;
- Deliberate propagation of computer viruses;
- Use of the internet to advertise, sell or purchase illegal materials and or services;
- Soliciting, responding to or discussing any illegal actions over the internet; • Unauthorised monitoring of electronic communications;
- Intentional unauthorised copying of copyright protected material or infringement of license agreements and other contracts;
- Violation of the privacy of individuals or entities that are creators, authors, users or subjects of the information resources.

Copyright

Copyright exists on all kinds of materials available on the internet, including web pages, software, gopher files etc. and any emails which may contain copyright material. Employees are expected to respect and adhere to regulations regarding copyright and other intellectual property rights. In the absence of permission or waiver statements, it is advisable to obtain permission before downloading or printing.

Confidential information

While technological systems can be relied upon to assist in maintaining confidentiality, they cannot ensure confidentiality. As stated above, users should therefore carefully consider the intended audience, tone, formality and format for all communications.

Retention and security of messages

Email messages and items stored on Council's computer system remains the property of Council. This includes items stored on desktop or notebook PCs. They may have the same legal effect as that of traditional hard copy documents.

Accordingly, all email messages should be treated as though others may later view them and these messages should be created with the same care that one would use in creating hard copy documents.

Email usage must be able to withstand public scrutiny. Users must comply with all applicable legislation, regulations, policies and standards. This includes complying with copyright and license provisions with respect to both programs and data.

Users need to be aware of policies regarding the retention of email or other records and any storage limits. Retention of paper copies of emails is expressly discouraged, unless the data needs to be recorded in a paper filing system.

ACCOUNTABILITIES & RESPONSIBILITIES

The Council is accountable for:

- Ensuring the organisation has in place a lawful, transparent and accountable policy framework, supported by a suite of compliant and appropriate policies and procedures.
- Endorsing (or not) each organisational policy document in a timely and effective manner; and
- Delegating implementation of each policy document to the CEO.

The CEO is accountable for ensuring the development, implementation, monitoring and review of this policy document, in accord with governing legislation and Council directives.

The Executive Management Team and Managers are responsible for:

- Ensuring that all workers under their direction comply with this policy document; and
- Enacting process to redress non-compliance with this policy document.

All workers are individually responsible for complying with this policy document.

GUIDELINES

Local Government Act 1995

Employee Code of Conduct

STATUTORY ENVIRONMENT

Local Government Act 1995

Record of Policy Review					
Version	Author	Council Adoption	Resolution	Reason for Review	Review Date
01	Nicole Gibbs	28/09/2023	72-23/24	New Policy	09/2025