Council Member Electronic Communications Policy

Reference Number:	1.9
Type:	Council Policy
Category:	Council Members
Relevant Community Plan Outcome:	• Our values, leadership and collaborative approach are bold and courageous and enables us to deliver value for our Community and Create a leading liveable City
Responsible Officer(s):	Manager Information Services
First Issued/Approved:	December 2000
Minutes Reference:	CoS 03/04/2023, Item 4.17
Last Reviewed:	April 2023
Next Review Due:	April 2025
Applicable Legislation:	Local Government Act 1999 Broadcasting Services Amendment (Online Services) Act 1999 Electronic Transactions Act 2000 Equal Opportunity Act 1984 Copyright Act 1968 Privacy Act 1988 National Principles for the Fair Handling of Personal Information
Related Policies:	Use of Unauthorised Hardware and Software Policy Council Member Code of Conduct Policy Council Member Records Management Policy Media, Communications and Social Media Policy Mobile Device Policy (including BYOmD) – Council Members
Related Procedures:	Elected Member Technology – Conditions of Issue

1. Purpose

The City of Charles Sturt recognises the need to embrace new and emerging technologies to improve the way business is conducted and contribute to improving the way the City meets its business objectives.

Current and new electronic communication technologies provide opportunities for sharing information and conducting business. However, the use of electronic communication methods also requires the effective management of the associated risks to ensure a dependable and consistent communications environment and to protect the Council from commercial harm.

2. Scope

This policy applies to Council Members in their use of Council technology, equipment and services.

Council Members who use or access Council technology, equipment and/or services are bound by the conditions of this policy. This policy applies equally to equipment and facilities owned or operated by the Council.

3. Policy Statement

Electronic Communication includes but is not limited to:

- Internet sites and pages
- Electronic journals and texts
- Library catalogues
- Email
- Discussion lists and forums
- Online News groups
- Internet relay chat
- Council website
- Electronic newsletters
- Social Media
- Cloud Storage and File Transfer / Sharing data of all kinds

All material sent, received, forwarded or transmitted may from time to time be subject to monitoring or retrieval.

3.1 Policy Requirements

3.1.1 Personal Use

All use, personal and business, must be appropriate and lawful.

Technology equipment is primarily for Council's business use and must be used in accordance with the requirements set out in this policy. Council recognises that a prudent level of use of electronic services may occur, as with telephone calls, for private purposes.

Personal (non-Council) use of Council supplied equipment or services by elected members is not allowed under Section 78 of the Local Government Act 1999 unless the use is specifically approved by Council and the member has agreed to reimburse the Council for any additional costs or expenses associated with this use. Incidental private use of equipment and services provided to elected members is recognised and approved by Council.

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

If Council equipment and/or data is stolen or compromised, elected members are to contact IS Service Desk immediately via telephone.

3.1.2 Personal Mobile Devices

The Council does not accept responsibility for any loss of personal data, delays, non-deliveries, service interruptions, technical difficulties or malicious activity arising, whether directly or indirectly, out of a Council Member's use of Council's services and facilities on their own personally owned Mobile Device.

Council Member's accessing emails with personal Mobile Device must use devices that are receiving operating system updates, and such devices must be configured to receive automated updates as soon possible.

Personal Mobile Devices used to connect to Council services must be configured to automatically lock, and require authentication such as facial recognition, fingerprint scan or a pin code to unlock.

Personal Mobile Devices are only permitted to access sensitive Council information when protected via the Council's Mobile Device Management (MDM) platform or via Mobile Application Management (MAM).

3.1.3 Passwords and Password Confidentiality

It is prohibited for Council Member's to:

- share their password(s) with others;
- 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 except by explicit direction from the Manager Information Services.

Passwords are considered to be a Council Member's electronic authorisation on Council's computer systems. Individuals are responsible for the security and regular changing of their password(s).

Council Members are required to take reasonable precautions to ensure that their password is not known by any other party.

Council Member's should be aware that although access passwords and other protection methods are in place, there is a general level of "insecurity" for communications via the Internet and email.

Council Members are required to use the Multi-Factor Authentication (MFA) self-enrolment process to register their authentication device(s) and install the mobile authentication application or setup phone number verification. MFA provides enhanced security and is an effective way to protect Council's network from cyber-attacks if user credentials are compromised. Support for self-enrolment can be obtained by contacting the Service Desk.

3.1.4 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 a system's functionality is intended to keep the identity of the sender anonymous, such as feedback forums or electronic surveys.

3.1.5 Confidential Messages

Confidential information should be sent with caution. If assistance is required to transmit confidential information the Service Desk can assist.

Do not send highly confidential messages via the Internet or email. Always exercise care and discretion with electronic communications.

Email messages are perceived to be instant in nature and instantly disposed of. However, they may be retained by both the recipient and the sender until specifically disposed of. There may also be an additional backup facility that retains a copy of the file even if it is eliminated from the sender's and recipient's computers.

Improper statements can give rise to liability – personally and for Council. Council Members are advised to work on the assumption that messages may be sent, forwarded, or transmitted to someone other than the intended message recipient. Controlled or limited distribution of messages cannot be guaranteed. Accordingly, Council Members are advised to be very cautious about committing totally private, sensitive or confidential messages to electronic communication.

Council Members should also be aware that email messages, even if expressed to be confidential, may have to be disclosed in Court proceedings, Freedom of Information requests, or in investigations by the Ombudsman competition authorities and regulatory bodies. It may be necessary for Council's Information Services staff or third parties (under Court or regulatory body appointments) to retrieve and/or disclose electronic information and communications. Elected Members are also provided access to records held by Council in performance of their duty as an elected member.

3.1.6 Virus Protection

Virus infection is most prevalent in non-work related emails. This includes Malware (malicious software) and phishing (the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.) etc. Service Desk assistance should be sought for any doubtful attachments or for assistance with virus protection.

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

3.1.7 Confidentiality Clause

All emails issued from Council email accounts must contain Council's standard confidentiality clause.

> *"Warning – This email message is intended only for the addressee(s) and may contain information that is confidential, subject to legal or other professional privilege, or protected by copyright. If you have received this in error, please notify the sender by reply email and delete this email from your system. You are not permitted to use, reproduce or disclose the contents of this email. No representation is made that this email is free of viruses. Virus scanning is recommended and is the sole responsibility of the recipient. Thank you."*

The purpose of this message is to advise any unintended recipients of the confidential nature of the communication. Council's standard email template contains this confidentiality clause.

Standard signature clauses for elected members using Council's email system are applied and managed by the Manager Information Services and include an endorsement that:

"Communications, including opinions, expressed by elected members do not necessarily represent those of or endorsed by the Council."

3.1.8 Unlawful Activities

Council Members 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.

Unlawful activities are absolutely prohibited, including:

- gaining access to any material which is prohibited or potentially prohibited, pornographic, offensive or objectionable;
- engaging in any conduct which offends Federal or State laws and regulations;
- embarrassing, bullying or harassing (sexually or otherwise) another person;
- sending or forwarding any material which is defamatory, abusive, sexist, racist or otherwise illegal (see 3.1.9 below);
- acting outside of copyright legislation (see 3.1.10 below);
- circumventing any filtering or other content access device or software; and
- interfering with electronic records management information.

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

3.1.9 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, email and all forms of social media. A statement made electronically is, by its very distribution, published. A statement is also published if it is simply received electronically and forwarded on electronically. The Council is at risk of being sued for any defamatory material stored, reproduced or transmitted via any of our facilities. Likewise, an individual may also be sued. As such, care should be taken to ensure that comments made electronically are respectful, honest and have a tone of courtesy.

Council Members are not to participate in the communication of any defamatory message.

3.1.10 Copyright

Council Members 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 and must be adhered to.

It cannot be assumed that you can reproduce, print, transmit or download all material to which you have access. Usage of any material should comply with the copyright requirements, as any material reproduced outside permitted uses or without the permission of the owner may be unlawful and may result in legal action against you and the Council.

3.1.11 Records Management

Emails are Council correspondence and the corporate standards and records management requirements, practices and procedures applying to letters also apply to emails and any attachments.

All emails, other than those 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 (Content Manager) is to be used for this purpose.

A reply email, or confirmation of receipt of an email for important communication is recommended. This confirmation must then be added to Council's official records management system.

Note: Council systems automatically retains copies of all email communication sent and received via Council Member email accounts.

Further information on this topic is contained within the Council Members Records Management Policy.

3.1.12 Use of Non-Council Email

Council members conducting their role in council will only create or receive official email correspondence via Councils email system. I.e. Personal email accounts will not be used for council business.

3.2 Breach of the Conditions of this policy

In circumstances where a Council Member breaches conditions of this policy, Council reserves the right to restrict the use or access to the technology, equipment or services and to maintain that restriction at its discretion and may invoke other disciplinary action or sanctions under the Council Member Code of Conduct.

3.3 Indemnity by Council Members

The Council bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of Council Members in accessing or using these resources or facilities. Council Members indemnify the Council against any and all damages, costs and expenses suffered by the Council arising out of any 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.

4. Definitions

List of all key terms and acronyms that are used in the policy, and their definition.

Key Term – Acronym	Definition
Cloud Storage and File Transfer/Sharing	Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network (typically the Internet) and can also be used for file transfer/sharing. Non approved Cloud Storage of Council information is not permitted.
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 his or her trade, credit or reputation.
Email	A service that enables people to exchange documents or material in electronic form. It is a system that enables people to send and receive messages through their computers or other devices. Each person has a designated mailbox that stores messages sent by others.
Hack	To gain access into another's computer system or files by illegal or unauthorised means.
Internet	A global research, information and communication network providing services such as access to information, file transfer and electronic mail.
Material	Includes data, information, text, graphics, animations, speech, videos and music or other sounds, accessible electronically, including any combination or selection of any of these.

Key Term – Acronym	Definition
Mobile devices	A small, often handheld computing device typically having a touch style screen and/or a miniature keyboard which is light weight (e.g., mobile phones and tablets)
Multi-Factor Authentication (MFA)	MFA provides enhanced security for your user account. Each login from a network outside Charles Sturt (external network) to services protected by MFA (Such as Office 365, Teams and RDS) will require you to authorise using the Microsoft Authenticator Application. This notification will appear as a push notification on your phone with the option to Approve/Deny the login. This will appear as a popup message on your phone.
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 access to information and programs within their authority. Network security is controlled by Information Services staff and is overseen by the General Manager, Corporate Services.
Signature	A signoff clause which allows you to add your own name, title, Council contact details, personal email address, direct telephone number, etc. at the end of outgoing emails.

I confirm that I have received, read, understand and accept Council's Electronic Communications Policy and the conditions and instructions contained in it.

Signed: ……

Name: ……

Date: …….