Electronic communications policy

Classification	Policy
Strategic reference	Goal 4: Governance and organisational culture
Relevant legislation	Local Government Act 1999
Relevant documents	Code of Conduct for Elected Members Employee conduct policy
Responsible officer	Coordinator Executive Services
Date adopted	February 2021
Next review date	February 2024

1 Policy statement

Council staff and elected members must be efficient, economical and ethical in their use and management of Council resources. Electronic communication facilities, such as mobile phones, internet and email, are Council resources provided for the purpose of assisting staff and elected members in the proper discharge and performance of their legislative functions and duties. All Council staff and elected members have a responsibility to ensure their proper use.

This policy is fundamental to sound risk management. Council is required to regulate use of telecommunication assets, internet and email so that staff and elected members have a safe working environment and the Council is protected from commercial harm and exposure to liability. To achieve that, electronic messages sent, received, forwarded or transmitted will be subject to recoding, monitoring or retrieval.

Users should be mindful of security issues that may result in the sharing or wider dissemination or publication of electronic communications. Electronic communications, even if expressed to be confidential, may have to be disclosed in court proceedings or in investigations by competition authorities and regulatory bodies or in response to a freedom of Information application.

2 Definitions

Council Staff

Includes people employed by Council, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel offered access to the Council's resources.

Electronic messaging

Electronic messaging is a generic term encompassing all forms of electronic communication.

This includes text messages, voice mail, electronic document exchange (electronic fax), electronic data interchange, and multimedia communications such as tele/video conferencing and videotext.

It involves the electronic transmission of information as discrete electronic messages over computer-based data communication network or voice messages over a telephone network.

Electronic communications facilities

Includes, but not restricted to, telephones (including hard wired, cordless & mobiles), computers connected to any network or data circuit, email, facsimiles, internet and intranet, two way radios, and satellite communications equipment.

Email

Is a service that enables people to exchange documents or messages in electronic form. It is a system in which people can send and receive messages through their computers and mobile phones. Each person has a designated mailbox that stores messages sent by other users. You may retrieve, read and forward or re-transmit messages from your mailbox.

Facsimile/fax

Refers to a communication device that converts each picture element of black and white into an electric signal. These signals in turn generate a constantly changing electrical signal that is transmitted on a data circuit (or telephone line) to a receiving facsimile.

Hack

To attempt by illegal or unauthorised means to gain entry into another's computer system or files.

Internet

A global research, information and communication network providing services such as file transfer and electronic mail.

Intranet

Is an internal (restricted) network that uses Internet technology, accessed over a personal computer.

Radio

Refers to wireless electromagnetic means of point to many point communications.

System security

To protect the information on the Council's network there are prescribed controls giving authorisation and access to files and directories in the network. Each individual has a password which allows them access to information and programs within their authority. Network security is controlled by the Manager Corporate Services and reviewed by the Chief Executive Officer.

Smart phone applications

Employees issued with Iphones who access applications for non-business use shall reimburse all costs incurred by Council.

Telephones

Include (but not limited to) hard-wired desk telephones, cordless & mobile telephones.

Tablets

Portable electronic devices, usually with a mobile operating system and touchscreen display, that may be used as a mobile computer.

3 Purpose of this policy

The purpose of this policy is to ensure the proper use of Council's electronic communication systems by Council staff and elected members for their intended purposes without infringing legal requirements, Council policies or creating unnecessary business risk.

It aims to ensure Council staff and elected members understand the way in which Council electronic communication facilities should be used.

Council makes its electronic communication systems available to Council staff and elected members to enable efficient sharing and exchange of information in the pursuit of Council's goals and objectives.

4 Scope

This policy applies to all Council staff and elected members, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel offered access to the Council's resources.

All rules that apply to use and access of electronic communication facilities throughout this policy apply equally to facilities owned or operated by the Council wherever the facilities are located.

The permitted use of Council's electronic communication facilities must be consistent with other relevant laws, policies and practices regulating:

- copyright breaches and patent materials legislation;
- anti-discrimination legislation;
- the Spam Act 2003;
- Code of Conduct for Elected Members;
- Employee conduct policy;
- Practices regulating discriminatory speech and the distribution of illicit and offensive materials, particularly those that are violent, discriminatory, sexual or pornographic in nature.

5 Personal use

Electronic communication facilities are primarily provided for Council's business use and must be used in accordance with this policy. For Council staff, reasonable personal use, not including family members, of the Council's electronic communication facilities is permissible. However, personal use is a privilege, which needs to be balanced in terms of operational needs. Personal use must be appropriate, lawful, efficient, proper and ethical and in accordance with any Council direction or policy.

Personal use:

- should be infrequent and brief;
- should not involve activities that might be questionable, controversial or offensive, including gambling, accessing chat lines/rooms, transmitting inappropriate jokes or sending junk programs/mail;
- does not extend to sending non-business related written material to any political organisation;
- must not disrupt Council electronic communication systems; and
- Should not interfere with, or detrimentally affect, staff duties and responsibilities.

Elected members are not permitted to use electronic communications facilities provided by the Council for a purpose unrelated to the performance of discharge of official functions and duties, unless the use is approved by the Council and the elected member will reimburse the Council of any additional costs and expenses associated with the use.

Misuse can damage Council's corporate and business image, and intellectual property generally, and could result in legal proceedings being brought against both Council and the user. Council staff and elected members reasonably suspected of abusing personal use requirements will be asked to explain such use.

6 Passwords and password confidentiality

Council staff and elected members are not permitted to interfere with any password. It is prohibited for anyone 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 Corporate Services or Chief Executive Officer.

You may be required to disclose your password/s to the Manager Corporate Services or Chief Executive Officer.

7 Identity

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

8 Inappropriate/unlawful use

The use of Council's electronic communications system to make or send fraudulent, unlawful or abusive information, calls or messages is prohibited. Council staff or elected members who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to the Chief Executive Officer.

Any Council staff member or elected member identified as the initiator of fraudulent, unlawful or abusive calls or messages may be subject to disciplinary action, including under the relevant code of conduct, and possible criminal prosecution.

The use of hand-held mobile phones whilst driving is an offence under Australian road rules and Council will not be responsible for the payment of any fines incurred as a result of the unlawful practice.

All Council staff and elected members should be aware that it is illegal to record telephone conversations, unless it is authorised under the Listening and Surveillance Devices Act 1972.

Inappropriate use of electronic communication devices includes (but is not limited to):

- use of Council's electronic communications facilities to intentionally create, store, transmit, post, communicate or access any fraudulent or offensive information,
- accessing and/or distributing material that is violent, discriminatory, pornographic or sexually explicit material, or other offensive material;
- gambling activities;
- representing personal opinions as those of Council; and
- use contrary to any legislation or any Council policy.

Use of Council electronic communication facilities must not violate federal or state legislation or common law. It is unlawful to transmit, communicate or access any material, which discriminates against, harasses or vilifies colleagues, elected members or members of the public on the grounds of: gender; pregnancy; age; race (nationality, descent or ethnic background); religious background; marital status; physical impairments; HIV status; sexual preference or being transgender.

9 Use of internet/websites

It is inappropriate to:

- intentionally download unauthorised software;
- download files containing picture images, live pictures or graphics for personal use;
- download computer games;
- Visit inappropriate web sites including chat lines / rooms, on-line gambling, or violent, sexually explicit or pornographic web sites.

10 Use of email

Any opinions expressed in email messages, where they are not business related, should be specifically noted as personal opinion and not those of the Council.

In addition to inappropriate usage restrictions for electronic communication facilities mentioned above, email is not to be used for:

- non-business purposes – ie 'junk' mail;
- sending or distributing 'chain' letters, 'hoax' mail or for other mischievous purposes (spam). Only business related subscriptions are permitted;
- soliciting outside business ventures or for personal gain;
- distributing software which is inconsistent with any vendor's licence agreement; and
- unauthorised access of data or attempt to breach any security measures on the system, attempting to intercept any data transmissions without authorisation.

Council staff and elected members should take care in writing and sending emails and responding to emails. In particular the use of the 'reply all' option as a response to emails sent to groups should be well considered.

11 Security and confidentiality

Council staff and elected members should be alert to the fact that sensitive or personal information conveyed through electronic communication facilities cannot be guaranteed as completely private and secure. The potential exists for sensitive information to be read, intercepted, misdirected, traced or recorded by unauthorised persons unless it has been encoded or encrypted. Such practices are normally illegal, but there can be no expectation of privacy.

Email messages are often retained by individuals or within the corporate records system.

Passwords or personal identity number protection must be activated on all mobile electronic communication facilities such as mobile telephones and laptop/notebook/tablet computers that are vulnerable to theft.

Information regarding access to Council's computer and communication systems should be considered as confidential information and not be divulged without authorisation. Users are expected to treat electronic information with the same care as they would paper-based information, which is confidential. All such information should be kept secure and used only for the purpose intended. Information should not be disclosed to any unauthorised third party. It is the responsibility of the user to report any suspected security issues.

All emails sent must contain a disclaimer/confidentiality notice or a link to the disclaimer. The purpose of such a message is to impress on any unintended recipient notice of the confidential nature of the email. A copy of the disclaimer/confidentiality notice can be obtained from the Manager Corporate Services.

12 Virus protection

Council staff and elected members are not to import non-text files or unknown messages into the system without having them scanned for viruses. This refers to 'air gapping' of data onto the system via USB thumb drives and magnetic media.
Virus infection is most prevalent in non-work related emails. Council staff and elected members are not to open, view or attempt to read attachments of any description (eg games, screen savers, documents, executable files, zip files, joke files or other mails), unless users are confident of their integrity. If in doubt, the Manager Corporate Services should be consulted. Council's virus protection system scans all emails, however, vigilance is still required.

13 Defamation

It is unlawful to be a party to, or to participate in, the trafficking of any defamatory message. To defame someone, defamatory material, including words or matter, must be published which is or is likely to cause the ordinary, reasonable member of the community to think less of the defamed person (the plaintiff) or to injure the plaintiff in his or her trade, credit or reputation.

For the purpose of defamation law, "publication" is very broad and includes any means whatsoever that we use to communicate with each other, including electronic messaging. A message containing defamatory material made electronically is, by its very distribution, 'published'. A message containing defamatory material 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 its facilities.

14 Copyright

Council staff and elected members must have regard to rules of copyright. Council staff and elected members should not assume that they can reproduce, print, transmit or download all material to which they have access. Material reproduced outside permitted uses or without the permission of the owner may be unlawful and may result in legal action against the staff member or Council member and the Council.

15 Monitoring and breaches

Council may monitor, copy, access and disclose any information or files that are stored, processed or transmitted using Council's electronic communication facilities. Such monitoring will be used for legitimate purposes only (such as legal discovery) and in accordance with any relevant legislation and/or guidelines.

Council will undertake necessary monitoring, auditing and activities to ensure staff and elected members' compliance with the acceptable usage of electronic communication facilities.

Council staff and elected members who violate any copyright or license agreements are acting outside the scope of their employment terms and roles respectively, and will be personally responsible for such infringements.

Council staff and elected members who do not comply with this policy may be subject to disciplinary action, including termination of employment for Council staff, and subject to criminal or civil proceedings. Council staff and elected members should report breaches of this policy to their manager or Chief Executive Officer.

16 Record keeping

Electronic communications which are sent and received in the conduct of Council business are official records of Council and are required to be maintained in good order and condition under the State Records Act 1997.

17 Policy review

The effectiveness of this policy will be reviewed every three years or as necessary.

18 Further information

This document is available on Council's website www.southernmallee.sa.gov.au and at the principal office of the Southern Mallee District Council at Day Street, Pinnaroo SA 5304.

A copy of this document may be purchased from Council.