

**Electronic Communication
 Facilities Policy**

Policy Reference Number:	1.2
Classification:	General
First Issued/Approved:	February 2006 (Res. 284/2006)
Review Frequency:	After the general election – every 4 years
Last Reviewed:	12 August 2014 (Res 40/2015) 13 January 2015 (Res 269/2015) 11 April 2017 (Res 407/2017) 15 January 2019 (res 276/2019)
Next Review Date:	January 2020
Responsible Officer:	Chief Executive Officer
Applicable Legislation:	<i>Local Government Act 1999</i>
Relevant Policies:	
Related Procedures:	
Compliance Standard:	

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 telephones, Internet and E-mail, 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. The Council is required to regulate use of Internet and E-mail so that Council 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 may from time to time be subject to monitoring or retrieval. Users should be aware that, although there are access passwords and the like, there is general "insecurity" for communications via Internet and e-mail. 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.

Definitions

Electronic Messaging

Electronic Messaging is a generic term encompassing all forms of electronically mediated communication.

This includes electronic mail for text messages, voice mail, electronic document exchange (Electronic FAX), electronic data interchange (EDI), and multi media 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 (includes hard wired, cordless & mobiles), computers connected to any network or data circuit, E-mail (Component of electronic messaging), facsimiles, Internet & Intranet, two way radios, pagers (beepers) and satellite communications equipment.

E-mail

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. 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

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.

Pager

Refers to a small telecommunications device that receives short radio messages – generally used by people who are continually changing their location. Pagers 'beep' when a message is received.

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 his or her authority. Network security is controlled by the [IT/Senior Administration Officer] and reviewed by the Chief Executive Officer.

Telephones

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

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.

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
- Council's 'Code of Conduct'
- Practices regulating discriminatory speech and the distribution of illicit and offensive materials, particularly those that are sexual or pornographic in nature.

Personal Use

Electronic communication facilities are primarily provided for Council's business use and must be used in accordance with this Policy. Reasonable personal use, including by Elected 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 the Council staff and Elected Members' duties and responsibilities or detrimentally affect the duties and responsibilities of other Council staff and Elected Members.

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. Council has resolved (resolution 312/2017) to allow Elected Members access to applications to be placed on their Council provided iPads, by Council administration.

Passwords and Password Confidentiality

Council staff and Elected Members are not permitted to interfere with any password. It is prohibited for any one 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 Chief Executive Officer.

You may be required to disclose your password/s to the Deputy Chief Executive Officer upon request.

Identity

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

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 the Australian Road Rules and Council will not be responsible for the payment of any fines incurred. All Council staff and elected members should be aware that it is illegal to record telephone conversations, unless it is authorised under Listening and Surveillance Devices Act 1972. Inappropriate use 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, data or material

- including pornographic or sexually explicit material, images, text or other offensive material;
- gambling activities;
- representing personal opinions as those of the 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 impairment;
- HIV status; or
- sexual preference or transgender.

Use of Internet/Web Sites

It is inappropriate to:

- intentionally download unauthorised software;
- download files containing picture images, live pictures or graphics for personal use;
- download computer games, music files or accessing web radio or TV stations; and
- visit inappropriate Web sites including chat lines / rooms, on-line gambling, sexually explicit or pornographic web sites (as stated previously)

Use of E-Mail

Any opinions expressed in E-mail 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, E-mail is not to be used for (applicable to external & internal systems):

- 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 accessing of data or attempt to breach any security measures on the system, attempting to intercept any data transmissions without authorisation.

Care should be taken in responding to internal E-mails addressed to 'Everyone' as any responses sent by pressing the 'Reply to All' button will be addressed to ALL staff. As such, Council staff and Elected Members are advised to take care in writing emails. Individual replies should be directed to the sender using the 'Reply' button.

Security & 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. 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.

E-mail systems should not be assumed to be secure. Council staff and Elected Members are advised to exercise care and discretion. E-mail messages are perceived to be instant in nature and instantly disposed of. They are retained by both the recipient and the sender until specifically disposed of and then only usually into what is called a trash file. There may also be an additional back up facility which retains the message for a period of time. It is often stored on a network file server where it can be copied onto a back up tape as routine data protection. That back up tape is a copy of the file even if it is eliminated from the sender and recipient's computers.

Passwords or personal identity number protection must be activated on all mobile electronic communication facilities such as pagers, mobile telephones and laptop 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 outside the Council must contain a message to the effect that "*This document is strictly confidential and intended only for use by the addressee unless otherwise indicated.*" The purpose of such a message is to impress on any unintended recipient notice of the confidential nature of the Email. It will sometimes be appropriate to make the same statement for internal messages. [Council may include a disclaimer/confidentiality notice that is to be attached to all emails]

Virus Protection

Council staff and Elected Members are not to import non-text files or unknown messages into your system without having them scanned for viruses. Email attachments are common. Virus infection is most prevalent in non-work related emails. The majority of viruses are enclosed in chain letter or joke attachments. 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 they have been scanned for viruses.

Defamation

It is unlawful to be a party to or to participate in the trafficking of any defamatory message. To defame someone, a statement 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 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 its facilities.

Copyright

Not all information on the Internet is in the public domain or freely available for use without proper regard to rules of copyright. Much of the information is subject to copyright protection under Australian law, and by Australia's signature to international treaties, protected at international levels too. "*Use*" includes down loading, reproducing, transmitting or in any way duplicating all or part of any information (text, graphics, videos, cartoons, images or music) which is not in the public domain.

Council staff and elected members should not assume that they can reproduce, print, transmit or download all material to which they have access. Council staff and elected members have rights to use material consistently with the technology or the rights of the owner of the material. 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 elected member and the Council.

Monitoring & 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's Deputy CEO will undertake periodic monitoring, auditing and activities to ensure staff compliance with the acceptable usage of electronic communication facilities in reference to this policy.

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, and subject to criminal or civil proceedings. Council staff and elected members should report breaches of this policy to their manager.

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. Reference should be made to Council's Records Management Policy for the record keeping procedures to be used to properly record electronic communications.

FURTHER INFORMATION

This policy will be available for inspection at the Council offices listed below during ordinary business hours and available to be downloaded, free of charge, from Council's internet site: www.robe.sa.gov.au

Royal Circus, Robe SA 5276

Copies will be provided to interested parties upon request. Email council@robe.sa.gov.au

Any grievances in relation to this policy or its application should be forwarded in writing addressed to the Chief Executive Officer of Council.

POLICY REVIEW

This policy may be amended at any time and must be reviewed at least every four years since its adoption (or latest amendment).