Electronic Communication Facilities Policy

Version No:	3.0
Issued:	17 April 2007
Last Review:	June 2020
Next Review:	June 2022

Name of Council	Wudinna District Council
GDS40 File reference	5.8
Responsibility:	Strategic Management
Policy Level:	Discretionary
Minutes reference:	21 July 2020 10.6.5
Applicable Legislation:	Local Government Act 1999 (SA), Spam Act 2003 (Cwth), Electronic Communications Act 2000 (SA), Electronic Transactions Act 1999 (Cwth)' Electronic Transactions Act 2000 (SA), Freedom of Information Act 1991 (SA) Surveillance Devices Act 2016 (SA), State Records Act 1997
Related Policies:	Council's 'Code of Conduct' for Elected Members and Council Staff Record Management Policy Elected Members' Allowances and Support Policy Social Media Policy

INDEX

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

1. POLICY STATEMENT

Council staff and Council 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.

2. DEFINITIONS

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

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 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
Any electronic communications system used for Council business purposes, 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 & Extranet, two way radios, pagers (beepers),satellite communications equipment, cloud based and any other online operational platforms (examples include: Skytrust, Magiq, DACO, X Matters, iViss, FOIMS, etc).

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.

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

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.

Social Media
A wide range of platforms that allows online communities with common interests to connect, share and consume information, thoughts and ideas. (examples include Facebook, Twitter, Snapchat, Linkedin etc.)

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 Finance Manager and reviewed by the Chief Executive Officer.

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

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.

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:

a. copyright breaches and patent materials legislation;
b. anti-discrimination legislation;
c. the Spam Act 2003;
d. Council's 'Code of Conduct'; and
e. practices regulating discriminatory speech and the distribution of illicit and offensive materials, particularly those that are 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 of the Council's electronic communication

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

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:

a. shall be allowed in specific circumstances as provided for in an employment contract;
b. should be infrequent and brief;
c. 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;
d. does NOT extend to sending non-business related written material to any political organisation;
e. must not disrupt Council electronic communication systems; and
f. should not interfere with the Council staff duties and responsibilities or detrimentally affect the duties and responsibilities of other Council staff.

Elected Members are not permitted to use electronic communications facilities provided by the Council for a purpose unrelated to the performance or discharge of official functions and duties, unless the use is approved by the Council and the Elected member agrees to reimburse the Council for 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 & 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 Chief Executive Officer.

Passwords are required to be changed monthly and must be a minimum of 8 characters, including a Capital Letter, Number and Symbol

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

All devices must have 'lock' settings if left unattended for a period of time and a password must be entered to re-activate the device.

7. IDENTITY

No e-mail 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.

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

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 handheld 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 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 Surveillance Devices Act 2016.

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.

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, 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).

10. USE OF E-MAIL

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 (applicable to external & internal systems):

- 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.

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

Care should be taken in responding to internal emails addressed to 'everyone' or "all staff" 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.

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. 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 backup 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.

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.

All Council staff and Elected Members are required to read, understand and sign as having agreed to the IT Security Procedure and Agreement form prior to using a Council provided email facility.

12. VIRUS & MALICIOUS ATTACK 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 e-mails containing links from illegitimate banking organisations, chain letter or joke attachments.

Council staff and Elected Members are not to open, view or attempt to read attachments of any description (e.g. games, screen savers, documents, executable files, zip files, joke files or other mails), unless they have been scanned for viruses by up-to-date anti-virus & malicious attack software.

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.

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

14. 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 downloading, 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.

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's Chief Executive Officer will undertake periodic monitoring, auditing and activities to ensure staff and Elected Members' 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 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. Reference should be made to Council's Records Management Policy for the record keeping procedures to be used to properly record electronic communications.

17. AVAILABILITY OF POLICY

This Policy will be available for inspection at Council's principal office during ordinary business hours and on the Council's website www.wudinna.sa.gov.au. Copies will also be provided to interested members of the community upon request, and upon payment of a fee in accordance with Council's Schedule of Fees and Charges.

	Electronic Communication Facilities Policy	Version No:	3.0
		Issued:	17 April 2007
		Last Review:	June 2020
		Next Review:	June 2022

APPENDIX

All staff are required to sign the IT Security Procedure & Agreement for their personnel file.

Wudinna District Council

IT Security Procedure & Agreement

As part of your employment with Wudinna District Council, you have access to passwords and security codes which must be kept secure and confidential at all times.

This agreement clarifies procedures that you must follow when accessing Council systems.

- Security Codes – do not write these down or give them to anyone outside of the organisation
- Passwords – these need to be complex: minimum of 8 characters including Capital Letter, Number and Symbol. You will be required to change these regularly: PC's and Mobile Devices to be changed monthly.
- PC's and Mobile Devices – these should have settings to sleep/lock after a period of time and request password entry to re-open.
- Mobile Devices – need to be kept secure at all times, do not allow anyone outside of the organisation to access devices.

Computers

Each month you will be prompted to change your Password.

This will need to be a 'complex' password which means it must contain a minimum of 8 characters and of these, at least one must be a Capital Letter, a Number and a Symbol.

Example Only (DO NOT USE THIS): Wudinna/01

Please ensure the password is not easily guessed by people outside the organisation.

Do not give the password to people outside the organisation and don't write it down.

Mobile Devices

This includes mobile phones, tablets etc.

Must be kept secure at all times.

Do not share access to Council devices or personal devices that have access to Council's system.

Ensure the device has settings to sleep/lock if unused for a period of time (this could be as little as a minute or two).

Ensure the device has settings to ask for a passcode to open each time it is used.

Most mobile device passcodes are often only a 4-6 digit number, please make sure it is a more 'complex' passcode eg not 123456, 000000, 5652 or 1925.

You will not be prompted to change this passcode by the device (unless it has that option in the settings) therefore you will need to manually change the passcode yourself, this could be done when changing the PC password each month.

Laptops

To use a Council laptop, you will require the same Username and Password you use to log onto your desktop PC.

As this Username is connected to your PC, the password will change each month when you change it on the PC.

IT staff will ensure Council laptops have the sleep/lock access and request passwords to unlock.

I agree to the above conditions and agree to abide by all security measures to ensure the safety of Wudinna District Council's systems.

Name _____

Position _____

Signature _____ Date: _____

Document Number 12.3.16.4.15 Version 1 Issued 16 February 2018