

	<i>Electronic Use Policy</i> Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

1. Purpose

The purpose of this policy is to ensure the proper use of Council's electronic devices and communication systems by Council staff and Elected Members.

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.

2. Scope

This policy applies to all "Council staff" and "Elected Members" as defined in section 3.

All rules defined in this policy apply equally to all devices and systems owned or operated by the Council wherever they are located.

The permitted use of Council's electronic devices and communication systems must be consistent with other relevant legislation, policies and industry guidelines. Important reference documents can be found in section 6.

3. Definitions

Definitions not listed are to be taken as consistent with relevant legislation as referenced in section 6.

Staff	includes persons employed by the District Council of Grant, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel offered access to the Council's resources
Elected Members	includes persons that have been elected to represent the District Council of Grant for the current term, and, for this policy only, family members that have access to the systems issued to these elected members

4. Policy

Council staff and Elected Members must be efficient, economical and ethical in their use and management of Council resources. Electronic devices and communication systems, such as computers, telephones, Internet, programs, apps 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 and lawful use.

This policy is fundamental to sound risk management. The Council is required to regulate the use of electronic devices and communication systems, so that Council staff and Elected Members have a safe working environment and the Council is protected from commercial harm and meets its legislated obligations. Electronic communications, even if expressed to be confidential, may have to be

	Electronic Use Policy Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

disclosed in court proceedings or in investigations by competition authorities and regulatory bodies or in response to a Freedom of Information application. Care should always be taken to present a professional approach to all communications, internal and external. **All Council electronic devices and communication systems are subject to monitoring and management as required.**

4.1. Personal use

Electronic devices and communication systems are primarily provided for Council's business use and must be used in accordance with this Policy. For Council staff, reasonable personal use, including by family members, of the Council's electronic communication systems 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 material or sending junk programs/mail;
- does NOT extend to sending non-business related written material to any political organisation;
- must not disrupt Council electronic devices and communication systems; and
- must 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 devices and communications systems 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 Council 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.

Personal use of devices which are set up with data plans which have set limits will require payment of any additional charges for private use or for usage in another country where high data charges may apply.

	Electronic Use Policy Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

Before travelling overseas employees must turn data roaming off and seek advice from the Information Services section in relation to how to avoid data charges or arrange a pre-purchase of an applicable data package if required for Corporate use.

4.2. Security and Password Confidentiality

Users should be aware that, despite passwords and other authentication methods, electronic communications carry inherent insecurities. 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 either directly or indirectly e.g. by having passwords written down in obvious locations;
- Leave a device unlocked or unattended in an unsecured location;
- 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 CEO or relevant Director.

You may be required to disclose your password/s to the ICT Coordinator upon request. Always seek clarification from your supervisor if you are unsure of the validity of such a request.

4.3. Identity

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

4.4. Inappropriate/Unlawful Use

The use of Council's electronic devices and communication systems 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 Manager Human Resources and Community, or the Chief Executive Officer respectively.

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, and criminal prosecution. Council will not be responsible for any fines or penalties incurred due to an unlawful practice.

Inappropriate or unlawful use includes (but is not limited to):

- using mobile devices whilst driving;
- recording any conversation without all participants knowledge/ approval;
- transmit, communicate or forward any defamatory or inappropriate material, whether you believe it to be true or not;
- using Council's electronic communications systems to intentionally

	Electronic Use Policy Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

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;

- transmit, communicate or access any material, which discriminates against, harasses or vilifies colleagues, Elected Members or members of the public on the grounds of any protected attribute;
- cyber-bullying activities;
- gambling activities;
- representing personal opinions as those of the Council; and
- use contrary to any legislation or Council policy.

4.5. Use of Internet and Intranet

Authorised users may be granted access to internet services over the Council network subject to the requirements of their role within the Council.

The Council automatically filters internet access to internet services over its network and blocks access to individual websites or categories of internet content that it considers inappropriate.

Confidential or restricted information regarding the Council business practices and procedures or personal information about any Council staff, Elected Members, ratepayers, members of the public or contracting third parties should not be published on the Council internet or intranet sites, unless required by legislation.

It is inappropriate to:

- use Council resources or data in artificial intelligent services unless it is in line with Council's AI usage policies or procedures,
- download or install any software without authorisation from the ICT Coordinator;
- download large files such as those containing data, video, picture images, or graphics for personal use;
- stream non work-related video, music, web radio or TV stations other than to fulfill a specific purpose within the range deemed as acceptable limits of personal use;
- post on or access non-Council social media such as Facebook, other than to fulfill a specific purpose within the range deemed as acceptable limits of personal use;
- play online games; or
- visit inappropriate web sites including but not limited to shopping, gambling, or sexually explicit or pornographic sites.

There is no acceptable personal use limits for illegal or inappropriate content, sites or apps.

	Electronic Use Policy Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

4.6. 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 systems mentioned above, E-mail 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;
- sending Council data or information for non-business purposes including to staff personal E-mail;
- soliciting outside business ventures or for personal gain;
- distributing software which is inconsistent with any vendor's licence agreement; or
- unauthorised accessing of data or attempt to breach any security measures on the system, attempting to intercept any data transmissions without authorisation.

4.7. Use of USB Devices, external hard drives, Smart Phones and Cloud based storage programs for transporting Electronic Files

Unless otherwise authorised, staff are restricted from transporting Council's electronic records on external devices or cloud services due to the risk of virus/malware infection from computers not within Council's network.

All office staff have access to One Drive which should be used for storage of work-related files for use on Council devices or for sharing with external business users. Laptops and USB storage devices can be requested for all other work-related purposes from the ICT Coordinator.

4.8. Security & Confidentiality

Council staff and Elected Members should be aware that sensitive or personal information stored on electronic devices or conveyed through electronic communication systems 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. Confidential information such as passwords and credit card details should never be shared via E-mail or other electronic communication methods.

E-mail systems should not be assumed to be secure. Council staff and Elected Members are advised to exercise care and discretion. E-mails are backed up daily and retained on network file servers and transferred permanently onto backup tapes. E-mail communications may be subject to inspection or release under South Australian or Commonwealth legislation.

	Electronic Use Policy Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

Passwords or a PIN (personal identity number) protection must be activated on all transportable electronic devices where any Council material is stored such as mobile phones, tablets and laptop 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.

Council staff and Elected Members must either shut down or sign out of their computers at the end of the day. Council staff and Elected Members must also lock their computer desktop or log off when leaving their device unattended during the day (no matter the timeframe it is unattended for). It is recommended that any password protection options be turned on with the screen saver function on their desktop.

Ensure all files related to Council business are stored on the relevant network drives. These files should not be stored on desktops, documents, downloads, local drives e.g. C: drive or personal storage devices.

Council staff and Elected Members must be vigilant in reporting any changes in operation, error messages and problems experienced with their computers to the ICT Coordinator.

4.9. Virus Protection

Council staff and Elected Members are not to import unknown files or messages into Council systems without having them scanned for viruses. Malware is most commonly spread via E-mail attachments. Council staff and Elected Members are not to open, view or install files from email attachments unless they are certain of the source or have approval from the ICT Coordinator. Phishing reporting functions are available in Councils E-mail system.

4.12. 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 staff, Elected Member and the Council.

	Electronic Use Policy <i>Policy No. FINPOL 10</i>	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

4.13. Monitoring & Breaches

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

Council's ICT Coordinator will undertake periodic monitoring, of activities to check staff and Elected Members' compliance with 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.

All Council staff and Elected Members will be required to enter into an **Electronic Use Policy Agreement** (Form IT004) to acknowledge they understand their obligations under this policy.

Council staff and Elected Members who do not comply with this policy may be subject to disciplinary action, including termination of employment, usage or access restrictions and criminal or civil proceedings. Council staff and Elected Members should report breaches of this policy to their manager or the Chief Executive Officer.

4.14. 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. Reference should be made to Council's Records Management Policy and procedures to properly record electronic communications.

5. Responsibilities

All staff and Elected Members are responsible for using provided devices and services for their intended purposes only without infringing legal requirements, Council policies or creating unnecessary business risk.

Council's Director Corporate and Community and ICT Coordinator are responsible for ensuring the requirements of this Policy are met.

6. References

References to legislation and/or documents include as amended, supplemented, updated and/or augmented from time to time.

6.1. Legislation

Local Government Act 1999 (SA)
State Records Act 1997 (SA)

	<i>Electronic Use Policy</i> Policy No. FINPOL 10	Version No:	5
		Responsible Officer/s:	ICT Coordinator
		Classification:	Council
		Issued:	19 August 2013
		Next Review:	June 2029

Freedom of Information Act 1991 (SA)
Copyright Act 1968 (Cth)
Privacy Act 1988 (Cth)
Surveillance Devices Act 2016 (SA)
Cybercrime Act 2001 (Cth)
Spam Act 2003 (Cth)

6.2. Council Policies / Procedures

Caretaker Policy
 Records Management Policy and Procedures
 Behavioural Standards for Council Members (as legislated)
 Behavioural Management Policy (for Elected Members)
 Employee Code of Conduct
 Media Communication and Social Media Policy
 Mobile Phone Usage Policy
 AI Use Policy

7. Review

This Policy shall be reviewed by the District Council of Grant at a minimum, once within every four (4) year Council term (or on significant change to legislation or other matters which could affect this policy).

Adopted	19 June 2006	06189.2
Reviewed	7 April 2008	08102.2
Amended	19 August 2013	13090.1
Amended	6 June 2016	16067.4.1
Minor Formatting	4 May 2020	Governance Officer
Amended	14 June 2022	Management Team
Reviewed	15 September 2025	25151