

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

1. Purpose

The purpose of this policy is to ensure the proper use of Council's electronic devices and communication facilities 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.

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 facilities owned or operated by the Council wherever the facilities are located.

The permitted use of Council's electronic devices and 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;
- Council's 'Code of Conduct' for employees and elected members; and
- Practices regulating discriminatory speech and the distribution of illicit and offensive materials, particularly those that are sexual or pornographic in nature.

3. Definitions

3.1 Council 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.

3.2 Elected Members

Includes persons that have been elected to represent the District Council of Grant, and for this policy only also includes family members that have access to the facilities issued to these elected members.

3.3 Electronic Messaging

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

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

This includes but is not limited to: Email, IM (instant messaging), Fax, Voice-mail, 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.

3.4 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.

3.5 Electronic Devices

Includes, but not restricted to, computers of all types (eg Servers, Desktops, Laptops, etc), computer network devices and infrastructure (eg network switches, routers, wireless access points, etc) and mobile devices (eg tablets, smartphones, etc)

3.6 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 or electronic devices. 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.

3.7 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.

3.8 Hack

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

3.9 Internet

The Internet is a global system of interconnected computer networks to serve several billion users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (www), the infrastructure to support email, and peer-to-peer networks.

	<p><i>Electronic use Policy</i> <i>Policy No. FINPOL 10</i></p>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

3.10 Intranet

Is an internal (restricted) network that uses Internet technology, usually accessed via a computer or similar device connected to the internal computer network.

3.11 Radio

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

3.12 System Security

To protect the information on the Council's network there are prescribed controls giving authorisation and access to programs files and directories in the network. Each individual has a password which allows them access to a specific level of information, programs, and levels or modules with these programs; this access is specific to the individual's authority. Network security is controlled by the ITC Coordinator of Council and reviewed by the Director Finance and Community Services.

3.13 Telephones

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

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 facilities, such as computers, 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 computer resources, 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.

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

4.1 Personal use

Electronic devices and 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, including by 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 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 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 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 be required to pay any additional charges for private use or for usage in another country where high data charges may apply.

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 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 either directly or indirectly e.g. by having passwords written down in obvious locations;

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

- 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 ITC Coordinator.

You may be required to disclose your password/s to the ITC Coordinator upon 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 Organisational Development, or in Elected Members cases, the Chief or Deputy Chief Executive Officer.

Any Council staff member or Council 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 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 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;
- Cyber-bullying activities
- 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

	<p>Electronic use Policy Policy No. FINPOL 10</p>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

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.

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 Employees, Elected Members, ratepayers, members of the public or contracting third parties should not be published on the Council internet site or intranet site, unless required by legislation.

It is inappropriate to:

- download or install any software without authorisation from the ITC Coordinator;
- download large files such as those containing data, video, picture images, or graphics for personal use;
- stream 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 social media such as Facebook, Twitter other than to fulfill a specific purpose within the range deemed as acceptable limits of personal use;
- play online games
- visit inappropriate web sites including chat rooms, on-line gambling, sexually explicit or pornographic web sites (as stated previously).

4.6 Use of Email

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):

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

- 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.

4.7 Use of USB Devices/Smart Phones and Cloud based storage programs for transporting Electronic Files

Unless otherwise authorised, Employees are restricted from using USB’s, Smart Phones or cloud based software to transport Council’s electronic records due to the risk of virus/malware infection from computers not within Council’s network. Access is provided to specific Employees who have an identified business need. Access to files on USB’s can be provided to Employees by Information Services upon request.

Where a business need for cloud based transfer of information is identified, Dropbox is Council’s preferred software for the transfer of Corporate files to and from relevant contacts. If Employees require access to Dropbox, they must lodge a request with ICT Coordinator who will confirm the business need and arrange approval from the relevant Manager and CEO if appropriate.

4.8 Security & Confidentiality

Council staff and Elected Members should be alert to the fact that sensitive or personal information stored on or electronic devices or 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.

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

Passwords or a PIN (personal identity number) protection must be activated on all mobile electronic devices where any Council material is stored such as mobile telephones, tablets 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 warning similar to below. 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. Please advise the ITC Coordinator if this warning is not present in the footer of your emails.

WARNING: The contents of this email are confidential and may be subject to legal professional privilege and copyright. No representation is made that this email is free of viruses or other defects. Virus scanning is recommended and is the responsibility of the recipient. If you have received this communication in error, you must not copy or distribute this message or any part of it or otherwise disclose its contents to anyone.

4.9 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.

4.10 User Maintenance

Ensure that Desktop Computers are closed down at the end of each working day (unless specifically requested otherwise).

Ensure all files related to Council business are stored on the relevant network drives. These files should not be stored on desktops or local drives e.g. C: drive. Be vigilant in reporting any changes in operation, error messages and problems experienced with their computers to the ITC Coordinator.

4.11 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

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

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.

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 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 Council member and the Council.

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 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 ITC Coordinator will undertake periodic monitoring, auditing of 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 ITC Coordinator.

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

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 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.

4.15 Other Relevant Council Documents

- Council's Records Management Policy;
- Council's Codes of Conduct for Elected Members and Council staff;
- Council's Elected Members' Allowances and Support Policy.

5. Responsibilities

Council's Deputy Chief Executive Officer and ITC Coordinator are responsible for ensuring the requirements of this Policy are met.

6. Review

This Policy shall be reviewed by the District Council of Grant at minimum every four (4) years, within 12 months of a general election (or on significant change to legislation or other matters which could affect this policy).

Action:	Meeting Date:	Minute Reference:
Adopted	19 June 2006	06189.2
Reviewed	07 April 2008	08102.2
Amended	19 August 2013	13090.1
Amended	6 June 2016	16067.4.1

	Electronic use Policy <i>Policy No. FINPOL 10</i>	Version No:	1.0
		Responsible Officer/s:	Deputy CEO
		Issued:	19 August 2013
		Next Review:	Apr 2019

Electronic Use Policy Agreement

This policy outlines:

- The business purpose and ownership of all computer emails, hardware and software.
- Users responsibility not to use the system for commercial, political, illegal, immoral or unethical purposes (including harassment of any kind)
- Restricted personal use
- Security of Council information issues.

I acknowledge that I have read and understand the Electronic Use Policy. I agree to comply with this policy.

Name: _____ Signed: _____
Employee

Date: _____

Approved : _____ CEO	Date: _____
Noted: _____ ITC Coordinator	Date: _____
To be given to the Manager Organisational Development for placing in personnel files	