

| | |
|---|---|
| Policy Section: | 1. Corporate Governance |
| Policy Name: | Information Technology Support for Council Members |
| Classification: | Public – Council Policy |
| Adopted: | 22 January 2019 |
| Frequency of Review: | Biennial |
| Last Review: | January 2019 |
| Next Review Due: | January 2020 |
| Responsible Officer(s): | Governance Coordinator Team Leader Digital and Business Information Solutions |
| Policy and Code of Practice Manual File Ref: | CC10/2601 |
| Council File Reference: | CR18/81961 |
| Legislation Authority: | State Records Act 1997 Freedom of Information Act 1991 Local Government Act 1999 |
| Related Policies and Codes: | Council Members' Allowances and Benefits Induction for New Councils |
| Related Procedures: | Records Management Procedure for Council Members |

1. INTRODUCTION

- 1.1 Council Members must be efficient, economical and ethical in their use and management of Council resources. Electronic communication facilities, such as telephones, internet and email, that are Council resources are provided for the purpose of assisting Council Members in the proper discharge and performance of their legislative functions and duties. All Council Members have a responsibility to ensure their proper use.
- 1.2 This Policy is fundamental to sound risk management. The Council is required to regulate the use of Council resources and the Internet so that Council 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 be subject to monitoring or retrieval.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 1.3 Council Members should be aware that, although there are access passwords and other system security procedures, there is generally "insecurity" for communications via Internet and email. Electronic communications, even if expressed to be confidential, may have to be disclosed in court proceedings or in investigations by relevant authorities and regulatory bodies or in response to a Freedom of Information application.
- 1.4 The Council encourages all Council Members to:
 - 1.4.1 Use IT Services in a responsible manner while performing the business purposes of Council. Council seeks to put into practice its policies regarding the computer use of Council Members to safeguard the integrity of computers, networks, and data, either at Council facilities or elsewhere; and
 - 1.4.2 All Council Members are required to use IT Services in a manner that does not breach this Policy or any other Council policies; for example, policies relating to occupational health and safety, harassment or discrimination, or any State or Federal laws.

2. PURPOSE

- 2.1 The purpose of this Policy is to ensure the use of IT Services by Council Members for their intended purposes without infringing legal requirements, Council policies or creating unnecessary business risk.
- 2.2 It aims to ensure Council Members understand the way in which IT Services should be used.
- 2.3 Council makes its IT Services available to Council Members to enable efficient sharing and exchange of information in the pursuit of Council's goals and objectives.

3. DEFINITIONS

- 3.1 **Computer System.** Means all computers, networks, servers and other similar devices that are administered by the Council and for which Council is responsible.
- 3.2 **Council.** Town of Gawler.
- 3.3 **Electronic Communications Facilities.** Includes, but not restricted to, telephones (includes hard wired, cordless and mobiles), computers connected to any network or data circuit, email (Component of electronic messaging), facsimiles, Internet and Intranet, two way radios, pagers (beepers) and satellite communications equipment.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 3.4 **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 (facsimile FAX), electronic data interchange (EDI), and multi-media communications such as tele/video conferencing and videotext and social media such as Facebook and Twitter. It involves the electronic transmission of information as discrete electronic messages over computer-based data communication network or voice messages over a telephone network.
- 3.5 **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. 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.
- 3.6 **Hack.** To attempt by illegal or unauthorised means to gain entry into another's computer system or files.
- 3.7 **Internet.** A global research, information and communication network providing services such as file transfer and electronic mail.
- 3.8 **IT Services.** Means the Network Systems, Computer Systems, includes Electronic Communications Facilities and all applications, software and peripherals used in connection with the provision of information technology services by Council.
- 3.9 **Network Systems.** Includes voice, video and data networks, switches, routers and storage devices.
- 3.10 **System or Network Administrator.** Means an employee responsible for managing the operation or operating system environments of computers or network systems, respectively.
- 3.11 **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 managed by the Council Information and Communication Technology Services Team.
- 3.12 **Tablet.** A kind of mobile computer, usually having a touchscreen or pen-enabled interface.
- 3.13 **Telephones.** Include (but not limited to) hard-wired desk telephones cordless and mobile telephones.

4. SCOPE

- 4.1 This Policy applies to all Council Members.
- 4.2 This policy applies to use and access of electronic communication and computer equipment owned or operated by the Council.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 4.3 The use of Council's electronic communication and computer facilities must be consistent with other relevant laws, policies and practices regulating:
 - 4.3.1 Copyright breaches and patent materials legislation;
 - 4.3.2 Anti-discrimination legislation;
 - 4.3.3 The Spam Act 2003;
 - 4.3.4 Privacy and confidential matters;
 - 4.3.5 Code of Conduct for Council Members; and
 - 4.3.6 Practices regulating discriminatory speech and the distribution of illicit and offensive materials, including those that are sexual or pornographic in nature.

5. RIGHT OF PRIVACY

- 5.1 The IT Services provided by the Council are to further the operations and business objectives of the Council.
- 5.2 Council Members should note that any right to privacy is limited in anything created, stored, sent or received on the Network or Computer Systems.
- 5.3 The Council does not guarantee privacy or confidentiality to Council Members of the IT Services and there are specific issues that users must be aware of;
 - 5.3.1 Council does not guarantee the security of any data created, stored, sent or received by Council Members on the Network or Computer Systems from unauthorised use or access.
 - 5.3.2 In the process of performing normal systems/network management and auditing functions, Council reserves the right to view Council Members files or potentially confidential information contained within the IT Services system.

6. PROVISION OF INFORMATION TECHNOLOGY TO COUNCIL MEMBERS

- 6.1 Pursuant to Section 78 of the *Local Government Act* 1999, Council has considered and is satisfied that the following facilities and support are necessary or expedient for Council Members to assist them in performing or discharging their official functions and duties:
 - 6.1.1 Personal computer, tablet or other suitable device plus anti-virus software – for use at meetings and for document sharing from the Council including agendas, minutes and workshop papers (in lieu of hard copies)
 - 6.1.2 Official Council email address
 - 6.1.3 Data connectivity

7. PERSONAL USE OF COMMUNICATION FACILITIES

- 7.1 Reasonable personal use of a Council provided tablet is permitted subject to no additional cost to Council and in line with the virus protection section of this policy. Council provided tablets are not to be used for visiting inappropriate Web sites including on-line gambling, sexually explicit or pornographic web sites. If in doubt about any proposed use, a Council Member should seek advice from the Council CEO or delegated Manager/Team Leader.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 7.2 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 Members reasonably suspected of abusing personal use requirements will be asked to explain such use and may be liable to reimburse Council for any expense incurred by Council.

8. NETWORK SYSTEM USAGE

- 8.1 **Providing services.** Council Members are not permitted to use or access the IT Services to provide network or computer-based services to third parties without the prior permission of the CEO or delegated Manager/Team Leader.

- 8.2 **Disruption of service.** Deliberate attempts to disrupt the operation or degrade the performance of the IT Services are prohibited, and will result in disciplinary actions against the user(s) concerned.

- 8.3 **Business use.** The IT Services are not to be used or accessed for non-Council business purposes unless previous approval has been obtained from the CEO or delegated Manager/Team Leader.

- 8.4 **Use of copyrighted or licensed materials.** The copying or installation of software onto any part of the Network or Computer Systems without the prior permission of the CEO or delegated Manager/Team Leader is prohibited. Council Members are reminded that copying or installation of software may infringe copyright or other intellectual property rights, and may create a liability for the Council Member and the Council.

- 8.4.1 You may be asked to show a valid license agreement to ensure the legal use of software on Council computers. Contact the CEO or delegated Manager/Team Leader if you have any questions regarding licensing issues.

- 8.5 **Passwords and Password Confidentiality.** Council Members are not permitted to interfere with any Council provided password. It is prohibited for anyone to:

- 8.5.1 Share their Council provided password/s with others;
- 8.5.2 Log on using other people's credentials;
- 8.5.3 Hack into other systems;
- 8.5.4 Read or attempt to determine other people's passwords;
- 8.5.5 Breach computer or system security measures; or
- 8.5.6 Monitor electronic files or communications of others.

You may be required to disclose your password/s to the CEO or IT Department upon request.

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

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 8.7 **Inappropriate/Unlawful Use.** The use of Council's IT Services to make or send fraudulent, unlawful or abusive information, calls or messages is prohibited. Council Members who receive any threatening, intimidating or harassing telephone calls or electronic messages through IT Services should report the incident to the CEO as soon as practicable.
- 8.7.1 Any 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.
- 8.7.2 Council 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):
- 8.7.2.1 Use of Council's Electronic Communication System 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;
 - 8.7.2.2 Use of Council's IT Services facilities to achieve or promote political gains, for example, as part of an election campaign;
 - 8.7.2.3 Gambling activities except authorised Council social activities i.e. footy tipping;
 - 8.7.2.4 Representing personal opinions as those of the Council; and
 - 8.7.2.5 Use contrary to any legislation or any Council Policy.
- 8.7.3 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, Council Members or members of the public on the grounds of:
- 8.7.3.1 Gender;
 - 8.7.3.2 Pregnancy;
 - 8.7.3.3 Age;
 - 8.7.3.4 Race (including nationality, descent or ethnic background);
 - 8.7.3.5 Religious background;
 - 8.7.3.6 Marital status;
 - 8.7.3.7 Physical impairment;
 - 8.7.3.8 HIV status; or
 - 8.7.3.9 Sexual preference or transgender.
- 8.7.4 Use of Council provided Internet / Web Sites. It is inappropriate to:
- 8.7.4.1 intentionally download unauthorised software;
 - 8.7.4.2 download computer games; and
 - 8.7.4.3 visit inappropriate websites including on-line gambling, sexually explicit or pornographic web sites.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

8.7.5 Use of email. All Council Members are provided with a Council based email, which will need to be used for all Council related correspondence. This will ensure all Council information is captured and appropriately registered in the Council Records Management System (State Records Act 1997). Any opinions expressed in email messages, where they are not Council approved, 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 and internal systems):

- 8.7.5.1 non-Council purposes – including ‘junk’ mail;
- 8.7.5.2 sending or distributing ‘chain’ letters, ‘hoax’ mail or for other mischievous purposes (spam). Only Council related subscriptions are permitted;
- 8.7.5.3 soliciting outside business ventures or for personal gain;
- 8.7.5.4 distributing software which is inconsistent with any vendor’s license agreement; and
- 8.7.5.5 unauthorised accessing of data or attempt to breach any system security measures on the system or attempting to intercept any data transmissions without authorisation.

Care should be taken in responding to group emails as any responses sent by pressing the ‘Reply to All’ button will be addressed to ALL original recipients. As such, Council Members are advised to take care in writing emails. Individual replies should be directed to the sender using the ‘Reply’ button.

9. SECURITY & CONFIDENTIALITY

- 9.1 Council Members should become familiar with the tools each computer system provides for maintaining the security and confidentiality of information stored on it.
- 9.2 Council Members should be aware of computer viruses and other destructive computer programs, and take steps to avoid being their victim or unwitting vector. Adequate protection software will be installed or available on any Council provided computer/tablet.
- 9.3 Council Members should either shut down or logoff their computer at the end of their days’ duties and lock the computer desktop or log off when leaving the computer unattended during the day. It is recommended that the password protection option be turned on with the screen saver function on the desktop.
- 9.4 Council Members should be aware 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 may be illegal, but there can be no expectation of privacy.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

- 9.5 Email systems should not be assumed to be secure. Council Members are advised to exercise care and discretion. Email messages are perceived to be instant in nature. 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. Messages will be stored on a network file server where it is backed up as routine data protection. That back up is a copy of the file even if it is eliminated from the sender and recipient's computers.
- 9.6 Passwords or personal identity number protection must be activated on all mobile electronic communication facilities such as mobile telephones and laptop computers that are vulnerable to theft.
- 9.7 Information regarding access to Council's IT Services should be considered as confidential information and not be divulged without authorisation. Council Members 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 Council Members to report any suspected system security issues.
- 9.8 All emails sent outside the Council contains the following message:
- 9.8.1 *“This email is intended for the named recipient only. The information contained in this message may be confidential, legally privileged or commercially sensitive. If you are not the intended recipient you must not reproduce or distribute any part of this email, disclose its contents to any other party, or take any action in reliance on it. If you have received this email in error, please contact the sender immediately. Any views or opinions expressed in this email and any files transmitted with it are those of the author only and may not necessarily reflect the views of the Town of Gawler and do not create any legally binding rights or obligations whatsoever. Unless otherwise pre-agreed by exchange of hard copy documents signed by duly authorised representatives, contracts may not be concluded on behalf of the Town of Gawler by email. Please note that neither the Town of Gawler nor the sender accepts any responsibility for any viruses and it is your responsibility to scan the email and the attachments (if any). All email received and sent by the Town of Gawler may be monitored to protect the business interests of the Town of Gawler.”*
- 9.9 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.

10. SOFTWARE INSTALLATION

- 10.1 Only software obtained by the Council is to be installed or used on the Network or Computer Systems. All software products carry a licensing regulation, which determine the number of installations that an organisation is legally permitted to perform. Breach of these regulations imposes very high penalties and may result in imprisonment.

11. VIRUS AND MALWARE PROTECTION

- 11.1 The Council needs to be protected from the threat of software viruses and malware to ensure that the integrity and reliability of the Council's computer systems and data are maintained efficiently and effectively. Council Members should endeavour to apply the following procedures whilst being active on the Council's network:
- 11.1.1 All documentation or data being transferred via a CD/DVD, USB Memory Stick or other remote storage device to the Council's network or computer systems must be scanned before opening.
 - 11.1.2 Laptop and tablet computers should not be used to access the internet unless virus protection is up to date. Council Members who suspect that their Council supplied equipment may have become infected whilst offsite must not connect the equipment back into the Council computer network until it has been scanned by the Council IT Department.
 - 11.1.3 Council Members are not to import non-text files or unknown messages into the system without having them scanned for viruses. Email attachments are common. Virus and malware infection is most prevalent in non-work related emails. The majority of viruses and malware are introduced via hyperlinks within emails. Council Members are not to open hyperlinks from unknown or suspicious sources unless first checked by the IT Department.
 - 11.1.4 In an attempt to protect Council's network from virus activity all attachments that are executable, movie, music or picture oriented will be intercepted and quarantined on a platform where they are unable to execute. All such files will be deleted after 14 days. A message detailing what files have been blocked will be forwarded to the intended "recipient" of the email.

12. DEFAMATION

- 12.1 It is unlawful to be a party to or to participate in the distribution of any defamatory message. To defame someone, defamatory material, including words or matter, must be published which is or is likely to cause an ordinary, reasonable member of the community to think less of the defamed person or to injure the defamed person in his or her trade, credit or reputation.
- 12.2 For the purpose of defamation law, "*publication*" is very broad and includes any means whatsoever that people 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 (and a Council Member responsible) is at risk of being sued for any defamatory material stored, reproduced or transmitted via any Council facilities.

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

13. COPYRIGHT

- 13.1 Not all information on the Internet is in the public domain or freely available for use without 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.
- 13.2 Council Members should not assume that they can reproduce, print, transmit or download all material to which they have access. Council 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 a Council Member and the Council.

14. MONITORING & BREACHES

- 14.1 Council may monitor, copy, access and disclose any information or files that are stored, processed or transmitted using Council's IT Services. Such monitoring will be used for legitimate purposes only (such as legal discovery) and in accordance with any relevant legislation and/or guidelines.
- 14.2 Council's Team Leader Digital and Business Information Solutions will undertake periodic monitoring, auditing and activities to ensure Council Members' compliance with the acceptable usage of IT Services in reference to this Policy.
- 14.3 Council Members who violate any copyright or license agreements will be personally responsible for such infringements.
- 14.4 Council Members who do not comply with this Policy may be subject to disciplinary action and subject to criminal or civil proceedings. Council Members should report breaches of this Policy to the CEO.

15. RECORD KEEPING

- 15.1 Electronic communications which are sent and received in the conduct of Council business may be official records of Council that are required to be maintained in good order and condition under the State Records Act 1997. Council Members' emails will be stored appropriately, archived and where appropriate saved to EDRMS (Electronic Document Records Management System). Council's Records Management Policy sets out the record keeping procedures to be used to properly record electronic communications and completed corporate documentation.
- 15.2 All electronic communications to and from a Council Member acting in their role as a Council Member, which are official records in accordance with the Records Management Procedure for Council Members, are to be created and received through the Member's specifically created Council email address.

16. GUIDELINES FOR DETERMINING WHAT ARE OFFICIAL RECORDS

- 16.1 Any record created, sent, received, forwarded or transmitted by Council staff and/or Council Members in the performance and discharge of their functions and duties may be classified as official records. However, records that are merely transitory, ephemeral, personal or private in nature will fall outside the definition of “official records”.
- 16.2 The following guidelines relate to some common records which Council staff and Council Members may create, send, receive, forward or transmit. This is not an exhaustive list, they are provided to assist in assessing whether information in any format may constitute an official record under the State Records Act.
- 16.2.1 Records that have continuing value are to be incorporated into Councils Records Management System:
- 16.2.1.1 Council diary appointments / invitations.
 - 16.2.1.2 Drafts which document significant decisions, reasons and actions or contain significant information that is not contained in the final form of the records.
 - 16.2.1.3 Significant messages concerning Council business, which include directives, proposals, recommendations, definitions or interpretations, formal communications, final versions, policy documents or statements, formal minutes.
 - 16.2.1.4 Conversations that relay information or involve matters of significance to the conduct of Council business should be documented in an appropriate format (e.g. file note) (ie directives, proposals, recommendations, definitions or interpretations, policy or procedure implications).
 - 16.2.1.5 Lobbying correspondence or petitions having continuing value.
- 16.2.2 Documents with no continuing value that may be destroyed (not required for incorporation into the Council Records Management System).
- 16.2.3 Drafts where there is no continuing value (not required for incorporation into the Council Records Management System).
- 16.2.4 Duplicate copies of messages and documents (not required for incorporation into the Council Records Management System).
- 16.2.5 Messages of routine instructions, private messages (not required for incorporation into the Council Records Management System).
- 16.2.6 Working papers (not relating to significant decisions) (not required for incorporation into the Council Records Management System).
- 16.2.7 Election materials or records created or received by a Council Member in regard to electioneering (not required for incorporation into the Council Records Management System).

INFORMATION TECHNOLOGY SUPPORT FOR COUNCIL MEMBERS POLICY

17. REVIEW AND EVALUATION

The effectiveness of this Policy will be reviewed on a biennial basis.

The Chief Executive Officer will report to Council on the outcome of the evaluation and if relevant make recommendations for amendments, alteration or substitution of a new Policy.

The Policy will not be altered or substituted so as to affect a process already commenced.

18. FURTHER INFORMATION

Further information about this Policy can be obtained by:-

Telephone: 8522 9211
Email: council@gawler.sa.gov.au
Appointment: Town of Gawler Administration Centre, 43 High Street, Gawler East.
Letter: PO Box 130, Gawler SA 5118

19. AVAILABILITY OF POLICY

The Policy is available for inspection during ordinary business hours at the Council principal office, Town of Gawler Administration Centre 43 High Street, Gawler East or is available on the Council website at www.gawler.sa.gov.au.

A copy of this Policy will be provided to interested parties upon request, for a fee as contained in the Register of Fees and Charges.