Use of Council Resources and Electronic Communications Policy

District Council of Mount Remarkable

1. Background

1.1 Section 62 of the Local Government Act 1999 ("the Act") provides that:

(1) A member of a Council must at all times act honestly in the performance and discharge of official functions and duties.

(2) A member of a Council must at all times act with reasonable care and diligence in the performance and discharge of official functions and duties.

(3) a member or former member of a council must not, whether within or outside the State:

- *make improper use of information acquired by virtue of his or her position as a member of the council to gain, directly or indirectly, an advantage for himself or herself or for another person or to cause detriment to the council; or*
- *make improper use of his or her position as a member of the council to gain, directly or indirectly, an advantage for himself or herself or for another person or to cause detriment to the council; and*
- *must not disclose information or a document in relation to which there is an order of a council or council committee in effect under section 90 requiring the information or document to be treated confidentially.*

1.2 Section 109 of the Local Government Act 1999 ("the Act") provides that:

(1) An employee of a Council must all times act honestly in the performance of official duties.

(2) An employee of a Council must at all times act with reasonable care and diligence in the performance of official duties.

2. Objective

2.1 The District Council of Mount Remarkable ("the Council") is committed to ensuring that all Employees and Council Members are efficient, economical and ethical in their use and management of Council resources.

2.2 Council's facilities, plant, equipment, electronic communication and other facilities are provided for legitimate Council business. When using these resources, Employees and Council Members are responsible for ensuring that they are used in a way that complies with the legislation, the respective Behavioural Management Policy, Employee Behavioural Standards and administrative best practice.

2.3 This policy is fundamental to sound risk management. Council is required to regulate the use of Council resources and facilities so that Employees and Council Members have a safe working environment and so that Council is protected from commercial harm and exposure to liability.

2.4 This policy applies to all Employees, Council Members, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel offered access to Council's resources.

2.5 All rules that apply to use and access of resources and facilities throughout this policy apply equally to facilities and resources owned or operated by Council wherever such resources or facilities are located.

3. General Requirements

3.1 For Employees, depending on the circumstances and subject to approval from the Chief Executive Officer (or his / her delegate), employees may be able to use Council facilities, plant, equipment or other resources for limited or restricted personal use.

3.2 However, personal use is a privilege, which needs to be balanced in terms of operational needs. It must be appropriate, lawful, efficient, proper and ethical and in accordance with any Council direction or Policy.

3.3 Relevant considerations when determining whether personal use is appropriate include, but are not limited to -

3.3.1 whether the use conforms to the Council's Employee Behavioural Standards and any lawful and reasonable direction given to an employee;

3.3.2 the type of facility, plant, equipment or resource use;

3.3.3 the cost and impact (both direct and indirect) of private use (direct cost being the actual cost of the use, whilst indirect cost could include lost employee productivity);

3.3.4 the reason for the private use;

3.3.5 the extent / level of the private use (this includes both the volume of use and the time spent by the employee in private use);

3.3.6 the time of the private use (whether the use was inside or outside of the employee's regular hours);

3.3.7 whether the use has flow on benefits to Council; and

3.3.8 the risks attached to the use (an example of a risk is a computer virus or damage to an item of plant and equipment).

3.4 Council Members are not permitted to use Council resources and 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 Council and the Council Member agrees to reimburse Council for any additional costs / expenses associated with the use.

3.5 Misuse can damage Council's corporate and business image, intellectual property, plant, equipment and other resources generally and could result in legal proceedings being brought against both Council and the user.

3.6 Employees or Council Members reasonably suspected of abusing personal use requirements will be asked to explain such use.

3.7 For Employees, misuse or a breach of the personal use requirements may also be considered misconduct, a serious disciplinary offence that could result in dismissal.

3.8 Where an Employee or Council Member is in doubt as to the appropriateness of the use of Council facilities, plant, equipment or other resources, they should seek guidance from the Chief Executive Officer.

4. Council Plant, Equipment and Physical Facilities

4.1 Council plant, equipment and facilities are provided for legitimate Council business only and should not be used for personal purposes other than in duly authorised circumstances.

4.2 Council plant, equipment and facilities include, but are not limited to, depot and office facilities, plant, equipment and sundry minor plant items and tools. Examples include photocopying, printing and binding within the administration area and use of plant, wash down facilities, vehicle servicing areas, plant and tools in the Works area.

4.3 Where such plant, equipment or facilities are used, appropriate arrangements and authorisation must be received beforehand, and such use must not occur during normal working hours.

4.4 The applicable hire rates or user charges must be paid by the Employee in such circumstances unless otherwise agreed by the Chief Executive Officer as part of the authorisation.

5. Electronic Communications Facilities - General

5.1 Passwords, Security and Confidentiality

5.1.1 Employees and Council Members are not permitted to interfere with any password or security code and it is prohibited for anyone to:-

a. Share their password(s) or security code(s) with others;

b. Hack into other systems;

c. Read or attempt to determine other people's passwords or security codes;

d. Breach computer or network security measures; or

e. Monitor electronic files or communications of others except by the explicit direction from the Chief Executive Officer.

5.1.2 The Chief Executive Officer may require an Employee or Council Member to disclose their password(s) or security code(s) and they may make a confidential record of these for subsequent use.

5.2 Identity

5.2.1 No email or other communication can be sent which conceals or falsifies or attempts to conceal or falsify the identity of the author and/or sender.

5.3 Inappropriate / Unlawful Use

5.3.1 The use of Council's electronic communications system(s) to make or send fraudulent, unlawful or abusive information, calls or messages is prohibited.

5.3.2 Employees or Council Members who receive any threatening, intimidating or harassing telephone calls or electronic messages must immediately report the incident to the Chief Executive Officer.

5.3.3 Any Employee or Council Member identified as the initiator of fraudulent, unlawful or abusive calls or messages may be subject to action under the relevant legislative and policy provisions and possible disciplinary action (for employees) and criminal prosecution.

5.3.4 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.

5.3.5 Employees and Council Members should also be aware that it is illegal to record telephone conversations, unless it is authorised under the Listening and Surveillance Devices Act 1972.

5.3.6 Inappropriate use includes, but is not limited to:-

a. Use of Council's electronic communication 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;

b. Gambling activities;

c. Personal business or activities such as share trading or buying and selling using sites such eBay

d. Representing personal opinions as those of Council; and

e. Use contrary to any legislation or any Council Policy.

5.3.7 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 other Employees, Council Members or members of the public on the grounds of:-

a. Gender, pregnancy or age;

b. Race (nationality, descent or ethnic background);

c. Religious background or marital status;

d. Physical impairment;

e. HIV status; or

f. Sexual preference or transgender.

5.4 Security and Confidentiality

5.4.1 Employees and Council 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.

5.4.2 Email systems should not be assumed to be secure. Employees and Council Members are advised to exercise care and discretion. Email 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.

5.4.3 Passwords or personal identity number protection must be activated on all mobile electronic communication facilities such as pagers, mobile telephones and laptop computers that are vulnerable to theft.

5.4.4 Information regarding access to Council's computer and communication systems should be considered as confidential information and not be divulged without authorisation.

5.4.5 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.

5.4.6 All Emails sent outside the Council must contain the following signature, the purpose of such a message is to impress on any unintended recipient, notice of the confidential nature of the Email and it will sometimes be appropriate to make the same statement for internal messages.

5.4.7 The required statement should read:-

"The contents of this Email message may be confidential, may contain privileged information and/or be the subject of 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 are not the intended recipient of this communication, any perusal, use, disclosure, distribution or reproduction of this message or any part of it is unauthorised and strictly prohibited. If you have received this Email in error, please contact the District Council of Mount Remarkable on +61 8 8666 2014 or postmaster@mtr.sa.gov.au and delete the Email without making a copy. The District Council of Mount Remarkable further advises that in order to comply with its obligations under the State Records Act 1997 and the Freedom of Information Act 1991, Email messages sent to or received from Council may be monitored or accessed by Council staff other than the intended recipient."

5.4.8 Employees and Council Members should also be aware that most software used to operate electronic networks, including web servers, mail servers, gateways etc log transactions and communications. System Administrators are capable and may be specifically directed by the Chief Executive Officer to monitor the contents of Emails sent and received by the corporate network, internet use and sites visited. Awareness should also exist that automated systems may scan incoming and outgoing Email for known offensive words and phrases, and that such Email may be reported and delivered or may be blocked depending on the rules applied to the detection of words or phrases.

5.5 Defamation

5.5.1 It is unlawful to be a party to or to participate in the publishing 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.

5.5.2 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.

5.6 Monitoring

5.6.1 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.

5.6.2 Periodic monitoring, auditing and other activities are undertaken to ensure Employee and Council Member compliance with the acceptable usage of electronic communication facilities in reference to this policy.

5.6.3 Employees and Council Members who violate any copyright or licence agreements are acting outside the scope of their employment terms and roles respectively, and will be personally responsible for such infringements.

5.7 Copyright

5.7.1 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.

5.7.2 Employees and Council Members should not assume that they can reproduce, print, transmit or download all material to which they have access. Employees and 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 the Employee or Council Member and Council.

5.8 Record Keeping

5.8.1 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.

6. Telephones – Fixed, Mobile, Fax and Personal Mobiles

6.1.1 It is understood that there will be times and circumstances where private calls and text messages need to be taken and made during normal working hours.

6.1.2 In these circumstances, individual staff will ensure personal telephone calls and their duration are kept to a minimum in line with the expectations of a professional workplace.

6.1.3 Outgoing personal calls to STD, 1300, 1900 numbers are not permitted, except in exceptional circumstances and following approval from the Chief Executive Officer.

6.1.4 To contribute to office harmony, personal mobile phones are better switched to silent or vibrate when in the workplace, so as not to cause disruption to other employees.

6.1.5 In all cases, the use of Mobile Phones, whether Council provided or personal, whilst driving or operating Council plant, equipment or vehicles is prohibited unless a hands free kit (which meets all necessary Australian and other applicable Standards and legal requirements) is being utilised.

7. Computer, Internet and Email

7.1 Internet & Web sites

7.1.1 It is inappropriate to:-

a. Intentionally download unauthorised software;

b. Download files containing picture images, live pictures or graphics for personal use;

c. Download computer games, music files or accessing web radio or TV stations; and

d. Visit inappropriate Web sites including chat lines / rooms, on-line gambling, on-line trading, sexually explicit or pornographic Web sites (as stated previously).

7.2 Email

7.2.1 Any opinions expressed in Email messages, where they are not business related, should be specifically noted as personal opinion and not those of Council.

7.2.2 In addition to the inappropriate usage restrictions already outlined within this Policy, Email (applicable to both internal and external systems) is not to be used for:-

a. Non-business purposes i.e. not junk mail;

b. Sending or distributing 'chain' letters, hoax mail or for other mischievous purposes (eg spam). Only business related subscriptions are permitted;

c. Soliciting outside business ventures or for personal gain;

d. Distributing software which is inconsistent with any vendor's licence agreement; and

e. Unauthorised access of data or attempt to breach any security measures on the system, attempting to intercept any data transmissions without authorisation.

7.3 Virus Protection

7.3.1 Employees and Council Members are not to import non-text files or unknown messages into their system without having them scanned for viruses. Email attachments are common. Virus infection is most prevalent in non-work related Emails, with the majority of viruses being enclosed in 'chain' letter or joke attachments. Employees and Council 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.

8. Breaches

8.1.1 Employees and Council Members who become aware of breaches of this Policy should report the breach to the Chief Executive Officer at the earliest opportunity.

8.1.2 Cases where the alleged breach involves the Chief Executive Officer shall be reported to the Principal Member.

8.1.3 Any alleged breach will be confidentially investigated to determine the substance of the allegation(s) in accordance with the principles of natural justice.

8.1.4 Employees and Council Members who violate any copyright or license agreements are acting outside of their employment terms and roles respectively and will be personally responsible for such infringements.

8.1.5 Employees and Council Members who do not comply with this Policy may be subject to disciplinary action, including termination of employment, for Employees, and subject to criminal and / or civil proceedings.

9. Document administration and control

Policy title:	Use of Council Resources and Electronic Communications Policy
Policy number:	04.14
Policy type:	Council / Governance
Responsible officer:	Director – Community & Corporate
First issued / adopted:	10 July 2007 reference 171-2007
Review period:	Within 12 months after the conclusion of a periodic election, inline with legislative changes or by resolution of Council
Last reviewed:	18 May 2021, 103-2021] January 2023 [010-2023]
Next review date:	By November 2027
Version:	Version 5
Date revoked:	n/a
Applicable legislation:	Local Government Act 1999 Behavioural Standards for Employees (only applicable if standard is endorsed by Council) Council Members Behavioural Requirements State Records Act 1997 Freedom of Information Act 1991 Listening Devices and Surveillance Devices Act 1972 Road Traffic Act 1961 and Australian Road Rules
Related documents:	Records Management Policy 04.43
Public consultation required / undertaken:	No
Availability	This Policy is available for inspection at the Council office and any person may obtain a copy of this Policy upon payment of the fee fixed by Council in accordance with Council's Fees and Charges adopted each financial year. It is also available on Council's website mtr.sa.gov.au. Any grievance in relation to this policy or its application should be forwarded in writing to the Chief Executive Officer of the Council.
File reference:	W:\4. Policy Manuals\Current Policy Manual