Elected Members Electronic Communications Policy	
	Council Policy
TRIM Reference	AR19/27728[v2]
First Issued	1 May 2006
Last Reviewed	11 July 2023
Next Review	November 2027

1. POLICY STATEMENT

Elected Members must be efficient, economical and ethical in their use and management of Council resources. Electronic Communication systems and resources, such as telephones, Internet and Email, are provided for the purpose of assisting Elected Members in the proper discharge and performance of their legislative functions and duties. Elected Members have a responsibility to ensure their legal and proper use.

2. PURPOSE

2.1 Purpose

The purpose of this policy is to ensure the legal and proper use of Council's electronic communication facilities, systems and resources by Elected Members. It aims to ensure Elected Members understand the way in which Council electronic communication facilities, systems and resources should be used, to enable efficient sharing and exchange of information in the pursuit of Council's goals and objectives.

2.2 Scope

2.2.1 This policy applies to the Mayor and all Elected Members granted access to Council resources.

2.2.2 All rules that apply to the use and access of electronic communication systems and resources throughout this policy apply equally to facilities owned or operated by the Council wherever the facilities are located.

2.3 Strategic Reference

5 Governance and Financial Sustainability
5.5 We meet or exceed legislative and accreditation requirements for all relevant programs.

3. PRINCIPLES

3.1 General Principles

3.1.1 The permitted use of Council's electronic communication facilities, systems and resources must be consistent with other relevant laws, policies and practices to ensure legal and proper use.

3.1.2 The use of Internet and E-mail is controlled and regulated so that Elected Members have a safe working environment and the Council is protected from operational and commercial harm and exposure to liability. As a result, electronic messages sent, received, forwarded or transmitted using Council resources are subject to monitoring and/or retrieval.

3.2 Personal Use

3.2.1 Electronic resources are provided to Elected Members for the performance or discharge of official functions and duties, in accordance with this Policy. Personal use is a privilege and use must be lawful, efficient, proper and ethical and in accordance with any Council direction or policy.

3.2.2 Personal use must:

a) not consume excessive data

b) not involve inappropriate or unlawful use (refer 3.4)

c) not extend to sending non business-related written material to any political organisation

d) not interfere with the performance or discharge of official functions and duties.

3.2.3 Misuse can damage Council's corporate image and intellectual property and could result in legal proceedings being brought against both Council and the user. Elected Members suspected of abusing personal use requirements will be required to explain such use.

3.3 Passwords and Password Confidentiality

3.3.1 Elected Members are not permitted to interfere with any password, and must not

a) share their password/s with others

b) hack into other systems or resources

c) read or attempt to determine other people's passwords

d) breach or attempt to circumvent computer or network security measures

e) monitor electronic files or communications of others.

3.4 Inappropriate/Unlawful Use

3.4.1 The use of Council's electronic resources to make or send fraudulent, unlawful or abusive information, calls or messages is prohibited. Any Elected Member who does not comply with the Policy will be subject to disciplinary action, under the relevant Code of Conduct, and possible criminal or civil proceedings.

3.4.2 Elected Members who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to the Mayor or Chief Executive Officer.

3.4.3 Inappropriate use includes (but is not limited to):

a) intentionally creating, storing, transmitting, posting or accessing any fraudulent communication or offensive information, data or material (including pornographic or sexually explicit material, images, text or other offensive material)

b) gambling activities

c) representing personal opinions as those of the Council

d) use contrary to any legislation or any Council policy.

e) intentionally download unauthorised software

f) downloading files containing picture images, live pictures or graphics for personal use

g) downloading computer games, music files or accessing web radio or TV Stations

h) visiting inappropriate Websites including chat lines/rooms on-line gambling, sexually explicit or pornographic websites.

i) activities considered to be circumventing security, hacking or of any intelligence gathering nature

3.5 Use of Email

3.5.1 Any opinions expressed in Emails, where they are not business related, should be specifically noted and specifically highlighted as personal opinion and not those of the Council.

3.5.2 Electronic "viruses" can be transferred via email and any imbedded programs and/or files. Any material from suspect sources should be treated in a cautious manner and reported to the Manager Information Systems and Records prior to their opening and use.

3.6 Intranet Access

3.6.1 Elected Members will not be provided access to internal information databases.

3.7 Security & Confidentiality

3.7.1 Personal information conveyed through electronic resources cannot be guaranteed as completely secure and 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.

3.7.2 Users should be aware that even with passwords, there is general "insecurity" for electronic communications, and items expressed to be confidential, may have to be disclosed in court proceedings, investigations, or under the Freedom of Information Act.

3.7.3 Email systems should not be assumed to be fully secure. Elected Members are advised to exercise care and discretion. E-mail messages are retained by both the recipient and the sender until specifically disposed of under the Records Management processes. There may also be an additional back up facility which retains the message for a period of time within the Council's electronic systems.

3.7.4 All Emails sent outside the Council must contain a disclaimer to the effect that "*This document is strictly confidential and intended only for use by the addressee unless otherwise indicated*". The purpose of such a disclaimer is to impress on any unintended recipient notice of the confidential nature of the E-mail.

3.7.5 The Manager Information Systems and Records will undertake periodic monitoring, auditing and activities to ensure Elected Members' compliance with the acceptable usage of electronic resources in reference to this policy.

3.7.6 Elected Members who do not comply with this policy may be subject to disciplinary action, including code of conduct investigations or criminal or civil proceedings. Breaches of this Policy must be reported to the Mayor or CEO.

3.8 Elected Member Devices

3.8.1 Elected Members who choose to use or purchase a device for the performance or discharge of official functions and duties, will be responsible for all operating costs for that device. Such devices will require the following:

3.8.2 If the non-Council issued device is not SIM based, access to emails will be provided via Outlook Web Access (OWA), with emails and any attachments to be downloaded to the device. A direct connection to the email server from a non-Council issued device is prohibited.

3.8.3 Non-Council issued devices will have access to the Internet Only Council Wifi whilst in the Council Chambers.

3.8.4 For non-Council issued devises, IT support will be limited to the initial set up of the device and only in relation to the Council installed software and email access. Any

other operating or functional issues with the device will need to be addressed by the Elected Member at their own expense.

3.8.5 For non-Council issued devises, Council will not be responsible for the integrity, security or usability of the device. The Manager Information Systems and Records reserves the right to remove all access to Council systems from non-Council devices deemed to be a cyber security risk or displaying attributes that constitute as a cyber security risk.

4. RESPONSIBILITY & REVIEW

4.1 Responsible Officer

The Manager Information Systems and Records is responsible for the review and application of this policy.

4.2 Availability

This policy will be available on Council's website

4.3 Review

This policy will be reviewed within 12 months of a General Election for Local Government, or as required to meet other obligations.

5. REFERENCES

5.1 Legislation

CyberCrime Act 2001
Evidence Act 1929
Freedom of Information Act 1991
Local Government Act 1999
Spam Act 2003
State Records Act 1997

5.2 Other References

Elected Member Behavioural Management Policy
Records Management Policy
Elected Member Records Management Policy
Staff Induction Form
Australian Cyber Security Centre 'Essential 8' Strategies