COUNCIL ACCEPTABLE USE POLICY

ECM DSID:	4422661
First Issued / Approved:	14 February 2023
Last Reviewed:	C140223/7338
Next Review:	14 February 2026
Responsible Officer:	**Manager, Information and Technology**
Date Placed on Webpage/ Intranet:	20 February 2023

1. PREAMBLE

1.1 Background

IT equipment and resources can enable work to be done more efficiently and effectively, however, users need to be mindful of security and similar considerations.

This policy is written to be consistent with the Information Security Management Standards ISO/IEC 27001:2015 and ISO/IEC 27002:2015.

1.2 Purpose

The purpose of this policy is to define the parameters of acceptable use in relation to Council's IT infrastructure and resources.

1.3 Scope

This policy applies to the use of any Council IT infrastructure and resources by all Elected Members, staff (including work experience placements and trainees), volunteers, and consultants and contractors across Council, including Alwyndor.

Where personal devices are used to access Council information, this policy will apply to the extent of Council-related business.

1.4 Definitions

Approved Council channels and tools means Council approved or Council issued IT infrastructure and resources.

Classification means identification of information and data as Public, Restricted or Confidential.

IT infrastructure and resources refers to computing, collaboration and communications equipment and systems, examples of which include telephones, facsimiles, mobile telephones, computers, tablets, printers, photocopiers, email, internet access, software, applications, networks, web services, cloud services, remote services and similar resources.

Users refers to people using IT infrastructure and resources covered by this policy, namely Elected Members, staff, volunteers, consultants and contractors.

1.5 Strategic Reference

The innovation focus area includes aspirations of creating conditions for early adoption and experimentation with beneficial technologies, and using digital tools to create transparency and enable direct participation.

2. PRINCIPLES

2.1 Council embraces the value that IT infrastructure and resources can add to the workplace and will provide all relevant users with appropriate tools to undertake their work effectively.

2.2 Users are expected to use all IT infrastructure and resources responsibly, with reasonable standards of professional courtesy, ethical conduct, cyber security and information privacy, following Council's values, all relevant laws and policies.

2.3 Council's information, systems and devices are to be used primarily for business purposes to further the interests of the community and the organisation. Nevertheless, users may use IT infrastructure and resources for incidental, limited personal use. This does not include for the purposes of carrying out private business/commercial activities (whether or not approved by the Chief Executive). Where personal use is deemed excessive, users may be requested to reimburse costs incurred.

2.4 Only approved Council channels and tools can be used. Where a user wishes to use IT infrastructure or resources that are not supplied by Council, permission must be sought via an IT request. This includes the use of personal devices for receiving/sending Council emails or other examples of Council information storage on personal devices.

2.5 Acceptable Use of Information

2.5.1 In addition to general responsibilities, when using Council information, users must:

- only use Council information for the purposes of Council business, in accordance with the classification of the information
- ensure appropriate classification of data
- use channels and tools appropriate to the classification
- exchange and store information only through approved Council channels and tools
- not disclose any information on the internet that is not classified as public
- notify IT of any suspected or known losses, thefts or breaches relating to information and data
- consider intellectual property rights and copyright when using information (including images) not created or owned by Council.

2.6 Acceptable Use of Systems

2.6.1 In addition to general responsibilities, when using Council systems, users must:

- keep their usernames and passwords confidential and not written down or saved anywhere in plain text
- log out or lock systems when not in use or unattended
- report suspected system breaches, including stolen or compromised passwords, and authorised system access
- requesting system access for new users and decommissioning of access for departing users is the responsibility of the relevant manager.

2.6.2 Users must not perform any activity that adversely affects the confidentiality, integrity or available of Council's information systems, networks and devices.

2.7 Acceptable Use of Devices

2.7.1 In addition to general responsibilities, when using Council issued devices, users must:

- store equipment in a safe environment
- inform IT if any malfunction or damage occurs
- immediately inform IT and their supervisor/ manager if a device is stolen or lost.

2.8 Acceptable Use of Messaging tools (Email, Teams, Sharepoint etc.)

2.8.1 Messaging tools are provided to Council employees for obtaining, sending and storing of information. Users of Council's messaging systems must ensure that all material made available, in any form whatsoever, appropriately represents Council. This includes but is not limited to:

- all users must use the messaging applications with respect and courtesy for others and in a responsible and professional manner and in accordance with the organisational values
- messaging tools are provided for work-related activities and the use of these for private use must be minimal
- work emails must not be forwarded to personal email addresses
- non-work related email addresses and telephone numbers must not be included in work related correspondence (with the exception of personal mobile phone numbers if approved for official use).
- users must ensure that any communication messages containing personal opinions on any subject are not sent to groups. Unsolicited messages containing personal opinions may have the potential to be misconstrued and can potentially offend
- all communications sent or received from Council's systems remain the property of Council

- consideration should be given to the appropriateness of email where other Council systems are better placed, particularly if communicating with large numbers of recipients or attachments are included.

2.8.2 Users are responsible for registering Council emails in the records management system for future reference.

2.9 Acceptable Use of the Internet

2.9.1 In addition to general responsibilities, when using Council systems, users must:

- take all reasonable care when downloading, accessing or executing files on or from internet services
- never disclose any usernames or passwords associated with Council on the internet. If accessing a site that requires a username and password, create a separate username and password that is completely different to your Council username and password
- carefully consider the type and nature of information requested when completing on-line application forms to ensure Council's information and network security are not compromised.

2.10 Other Security Considerations

2.10.1 Users must take reasonable care when downloading, accessing or opening files on or from internet destinations. This includes due care in completing on-line application forms. If in doubt about the security of a website, users should consult with IT.

2.10.2 Release of Council information into the public realm must be considered in the context of the Information Security Policy and the Social Media Policy.

2.10.3 Council may choose to block access to some sites, as well as record internet usage and sites visited. Access to these log files will be restricted to persons designated to perform relevant reporting and/or security controls.

2.10.4 Notwithstanding that emails may contain Council information, confidential information or material in which third parties own or claim copyright, Council may access, review, monitor, and disclose the contents of all messages created, sent or received using Council infrastructure (whether solely or in part) for the purpose of monitoring compliance with this policy or compliance with any terms and conditions of employment or engagement.

2.10.5 All reasonable care is taken to protect user privacy. However, the content of personal electronic communications, documents and data may be inspected with the authorisation of a General Manager where a valid business reason exists.

2.11 Unacceptable Use

2.11.1 Acceptable use expressly excludes use that is contrary to policy or legislation, excessive downloading and access to, and/or distribution/sharing of:

- sexually explicit material
- hate speech or offensive material
- material regarding violence, criminal and/or illegal activities
- material that aims to defame, discriminate or harass
- political lobbying
- operating a business
- peer to peer file sharing services
- sites or tools designed to scan for or exploit IT vulnerabilities
- material that violates copyright, trade secret, patent or other intellectual property rights
- material that infringes on the privacy of others
- material that may bring Council into disrepute.

3. REFERENCES

3.1 Legislation

Local Government Act 1999
State Records Act 1997

3.2 Other References

Information Security Policy
Social Media Policy
Mobile Device Policy
Elected Member Code of Conduct
Employee Code of Conduct
AS ISO/IEC 27001:2015
AS ISO/IEC 27002:2015
Fair Treatment Procedures
Managing Misconduct & Disciplinary Procedures
Workplace Relations Policy
Quality Working Culture Policy