Information and Communication Technology Acceptable Use Policy

Aligned City Value/s	**Approachable**	**Responsive**	**Transparent**	**Innovative**
Responsible Directorate	**Corporate Services**			
Responsible Business Unit/s	**Corporate Information Systems**			
Responsible Officer	**Chief Technology Officer**			
Affected Business Unit/s	**All Business Units**			

Objective

This Policy sets out the acceptable behaviour required by the City's technology users (the users) when using the City's Digital Assets.

The purpose of this policy is to:

- Define acceptable and unacceptable use of Digital Assets
- Reduce security, legal and operational risks
- Ensure responsible, ethical and lawful use
- Clarify consequences of misuse

Inappropriate use of Digital Assets may expose the City to cybersecurity risks, service disruption and legal issues.

Scope

This policy applies to all the City technology users (the users) using both City issued, and non-City issued computing devices that connect to the City's Digital Assets, at any location.

All the City's Digital Assets, including computer, phones, mobile devices, software, and network infrastructure together with access to the internet and email are provided primarily for business purposes. Limited personal use is permitted where it is lawful, incidental, does not interfere with work responsibilities, does not incur cost to the City, and does not breach this policy.

The use of these assets should therefore be consistent with that purpose.

Policy

Core Principles

All users must:

- **Use for business purposes:** Digital Assets must be used primarily to perform job responsibilities
- **Protect the City:** Use must not expose the City to risk, loss or reputational harm
- **Use approved systems:** Only authorised equipment, applications and services may be used
- **Act lawfully:** All use must comply with applicable laws and regulations
- **Maintain security:** Users must protect accounts, devices and information
- **Report issues:** Suspicious activity must be reported promptly

General User Responsibilities

- **Access and Use**: users may access Digital Assets for legitimate business and administrative purposes that align with the City's mission and objectives.
- **Collaboration and Sharing:** users may collaborate through City's approved tools and platforms, provided adherence to the City's policies and guidelines.
- **Personal Development:** users may access Digital Assets for personal development, such as skill-building, professional networking, or educational resources that are approved by the City.
- **Remote Access:** users may access Digital Assets remotely using the City's approved methods.
- **Usage of Personal Devices:** users are responsible for ensuring their devices are secure, updated and using the City's approved applications to connect to the City's network and systems.
- **Generative AI:** users may use approved generative AI tools for daily operations ensuring such usage is in accordance with the City's Generative Artificial Intelligence (AI) Policy.
- **Security and Incident Reporting:** users report suspicious activity, security incidents or system anomalies promptly.

Digital Assets Acceptable Use Principles

The examples below are not exhaustive. Any use that is unlawful, unsafe, unauthorised, inconsistent with City policies, or exposes the City to unacceptable risk may also be treated as unacceptable use.

Internet Usage

The City has provided internet and network services for internal communication, third-party communication, job-related browsing activity, and accessing internal services hosted in CoSi.

Unacceptable use includes the following:

Description
Using the internet for activities such as online gaming, dating and gambling.
Downloading software, music, movies etc.
Accessing pornographic or sexually explicit web sites.
Using any digital systems or devices in ways that pose a risk to child safety or conflict with the City's commitment to a child-safe environment.
Using the internet for commercial activities not directly related to the City.
Disclosing non-public information through websites, blogs, discussion forums etc.
Distributing copyrighted materials without permission, such as development code, music or video content.
Hacking into systems or accessing confidential information.
Using the internet to bully, harass, or discriminate against colleagues. This can include sending threatening emails or spreading false information.

Generative Artificial Intelligence (AI) Usage

The City has approved AI tools and has an Artificial Intelligence Policy to promote the usage of AI within the City.

Unacceptable use includes the following:

Description
Using AI tools/platforms not authorised by the City
Generating or distributing content through AI that promotes violence, hate speech, discrimination, or any form of harm to individuals or groups.
Using AI to generate harmful content that invades personal privacy, such as unauthorised sharing of personal data, confidential information, or sensitive details.
Using AI to create deceptive content for fraudulent purposes, including phishing, scamming, or impersonating individuals or organisations.
Generating realistic but fake images, videos, or audio recordings of individuals without their consent, which can be used for malicious purposes.
Using AI to create bots that engage in spamming, trolling, or other disruptive activities online.
Creating content that is sexually explicit, obscene, or otherwise inappropriate for the intended audience.

Email Services Usage

The City has provided email addresses to all its workforce.

Unacceptable use includes the following:

Description
Sending unauthorised marketing content or unsolicited email messages, includes “junk email” or “spam”.
Harassment through messages, including inappropriate language or tone.
Distributing or sharing confidential or sensitive material via e-mail to third parties.
Redirecting, forwarding, copying, or moving email containing City business information to your personal email addresses.
Inappropriately transmitting information which may violate the rights of others, including unauthorised text, images or programs, trade secrets or confidential property, trademarks, or service marks.
Signing up using City of Stirling mail address for non-business-related purposes
Sharing or disclosure of personal user identities, passwords, or security codes. Passwords must not be written down or left in a place where an unauthorised person might see them.

Microsoft 365 Collaboration and Storage Services

The City has allocated Microsoft M365 licenses to all its workforce to collaborate and share information with each other and outside the City.

Unacceptable use includes the following:

Description
Recording a meeting session without obtaining consent from participants.
Storing highly sensitive or personal identified information (PII) without proper authorisation and access controls.
Sharing data externally through M365 services without approval from the manager/data owner.
Failing to revoke access for external users when they no longer need to access data repositories.
Utilising the City’s cloud storage resources for personal needs.
Sharing personally identifiable or confidential information inappropriately or without due care.

Network & telephony

Unacceptable use includes the following:

Description
Making calls that are offensive, obscene, threatening, abusive or defamatory.
Use of telephones and corporate mobiles for commercial activities not directly related to the City.
Creating, introducing or distributing computer viruses or other malicious software onto the City's network device or system.
Unauthorised hacking or probing for security vulnerabilities in networks and systems.
Monitoring, intercepting or accessing network traffic, emails, files etc. intended for another person.
Users must not use personal or commercial VPN services to bypass City security controls or access City technology services.

Software and Application Usage

Unacceptable use includes the following:

Description
All types of software, applications, or subscription-based services must undergo a cyber risk assessment process prior to approval and use.
Software procured by or licensed to, the City should not be copied or distributed to the City's technology users. It should also not be re-used to un-licensed users in a way that violates the software's license policy. This includes computer software and cloud services.
Tampering with or disabling any installed security software (e.g. anti-virus software) from any City owned asset without prior authorisation. Installed security software must be kept always running.

Physical Security

Unacceptable use includes the following:

Description
Sharing devices issued by the City with friends, family or non-approved staff members.
Leaving devices issued by the City unattended in vehicles or public areas.
Leaving devices unlocked when left unattended.
Taking critical hardware offsite without prior authorisation.
Leaving materials containing non-public information unattended.

Exceptions

Any exception to the policy must be approved by the Chief Technology Officer (CTO) in advance.

Monitoring and Compliance

The City may monitor, log and audit use of Digital Assets for legitimate purposes including internal and external audits, security, compliance and operational integrity.

Failure to comply with this policy may result in:

- Access restrictions
- Training requirements
- Management or disciplinary action
- Referral under relevant Codes of Conduct

Definitions

Digital Assets means City-owned, City-managed or City-approved technology, systems, services, devices, accounts, software, applications, networks, data and digital content. This includes, but is not limited to, computers, laptops, mobile phones, tablets, servers, storage devices, email, internet, collaboration platforms, business systems, records, documents, images, audio, video and other digital information.

Microsoft 365 (M365) means cloud powered productivity platform (Office, Teams, SharePoint, and OneDrive).

Multi-Factor Authentication (MFA) means Multi-Factor Authentication methods required for additional cyber security, such as the Microsoft Authenticator App.

Personal Identified Information (PII) means any data that can be used to identify a specific individual which includes, Name, Date of birth, Physical address, Passport number, Email, Phone number etc.

Virtual Private Network (VPN) means a virtual private network that can provide a secure communications mechanism transmitted between networks.

Other relevant management practices/documents

The following information is not mandatory but informs and/or support the implementation of this policy:

Generative Artificial Intelligence (AI) Policy
Information Security Management Practice
Mobile Computing Device Management Practice
Data Roles and Responsibilities Management Practice
City of Stirling Code of Conduct
Elected Members, Committee Members and Candidates Code of Conduct
Social Media Management Practice
Integrity and Misconduct Management Practice

Legislation/local law requirements

State Records Act 2000
Local Government Act 1995
Freedom of Information Act 1992

Office use only				
Relevant delegations	Not applicable			
Initial Council adoption	**Date**	2 March 2010	**Resolution #**	0310/013
Last reviewed	**Date**	7 July 2026	**Resolution #**	0726/023
Next review due	**Date**	7 July 2028		