Information and Technology Acceptable Use Policy

Responsible Directorate	**Corporate Services**
Responsible Business Unit/s	**Corporate Information Services**
Responsible Officer	**Manager Information Communications and Technology**
Affected Business Unit/s	**All Business Units**

Objective

The objectives of this policy are to assist Users to make appropriate use of the City of Stirling's (City's) Information and Technology (IT) resources and to inform about the consequences of misuse. Inappropriate use exposes the City to risks including virus attacks, compromise of network systems and services and legal issues.

Scope

This policy applies to Users of the City's IT Resources.

The scope of this policy applies to the use of information, electronic and computing devices and network resources to conduct business or interact with internal networks and business systems owned or leased by the City. Users of IT are responsible for exercising good judgement regarding appropriate use of information, electronic devices and network resources in accordance with the City's policies and standards and local laws and regulations.

Policy

Overview

The City is committed to protecting its employees, partners and the organisation from illegal activity or damaging actions by individuals, either knowingly or unknowingly. As such everyone is aware that they are bound by the City's Code of Conduct which has provisions for the proper use of official information, equipment and facilities. This extends to ensuring that IT resources are used in a responsible and accountable manner that ensures the efficient, effective and acceptable use.

This policy is not meant to impose restrictions that are contrary to the City's established culture of openness, trust and integrity. Acceptable use requires sensible, ethical, efficient and legal utilisation of the City's IT resources.

All IT systems, including but not limited to computer equipment, software, operating systems, storage, telephony media and network infrastructure are the property of the City. These systems are to be used for business purposes in serving the interests of the organisation and of our customers in the course of normal business operations.

Effective information security is a team effort involving the participation and support of every User who deals with information and/or information systems. It is the responsibility of every User to know these guidelines and to conduct their activities accordingly.

The following overarching principles are to be adhered to by all Users with access to the City's systems or data.

Business first: IT assets and services are made available to personnel to perform their duties. Limited personal use is permitted provided it does not impact the performance of those duties.

Protect our interests: IT resources should not be used in a way that could cause the organisation embarrassment or loss, or to promote interests other than those of the City.

Approved components: Only authorised equipment, software, applications (apps) and services can be introduced and used in the City's environment.

Lawful Use: Company IT assets and resources can only be used for lawful activities, and cannot be used for any activities which would contravene any laws or regulations with which the City is obliged to comply.

Report Issues: If you see something that doesn't appear right, let us know. Security is everyone's responsibility.

Acceptable Use

Access to corporate systems and information is provided to approved users only. Users of City of Stirling ICT are permitted to use the systems for work related purposes and for limited personal use that does not interfere with their work or compromise the organisation (i.e. during lunch times or before and after work).

Acceptable Use involves:

- accessing only accounts, files, and data that are the employees own, that are publicly available, or to which the employee has been given authorised access;
- only accessing files, data, information, irrespective of their access privileges, where they have a valid business reason to do so;
- ensuring that only City owned IT hardware is connected to the City's network, unless authorised by the Manager ICT as per the Mobile Computing Device Management Practice;
- ensuring that mobile technology, such as phones and laptops etc., are appropriately secured;
- maintaining the confidentiality and privacy of information classified or known by the User as private or confidential and keeping such information in their possession secure;
- ensuring that confidential reports are not left on printers or in plain view on desks;
- not using City information for non-City related purposes;
- keeping confidential any passwords provided for access to City systems and not sharing these with other people or accessing any system under another User's sign on;
- not disclosing any information to which employees have access to and do not have lawful ownership, authority, or permission to disclose;
- reporting suspected policy violations to their Business Unit Manager or Director;
- ensuring the content and disclosure of communications is appropriate;
- using the City's computers and networks only for purposes that are legal and authorised;
- obtaining authority from the CIS business unit before installing any software or hardware;
- taking all reasonable steps to protect the City's systems or any stored information/data, by:
- not deleting data/information without cause;
- not creating or propagating viruses;
- not disrupting services or damaging files;
- use of authorised file sharing solutions;
- using only CIS provided encrypted USBs with COS infrastructure including desktops and laptops;
- ensuring computer workstations are left secure when not in use by signing-off and/or securing from unauthorised use;
- ensuring that all the user, generic, service, system, network and database accounts are secured using a strong password, and where possible using multifactor authentication (MFA).

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the City authorised to engage in any activity that is illegal under local, state or federal law while utilising City owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use - the following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City;
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City or the end User does not have an active license;
- Accessing data, a server or an account for any purpose other than conducting City business, even if the employee has authorised access;
- Exporting software or technical information, in violation of international, regional or local export control laws, is illegal. CIS should be consulted prior to the export of any material that is in question.
- Unencrypted transfer or storage on removable media of sensitive or confidential information as determined by the relevant data custodian. Use of removable media may be monitored
- Introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs etc.);
- Revealing account passwords to others or allowing use of their account by others. This includes family and other household members when working from home;
- Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the User's local jurisdiction;
- Making fraudulent offers of products, items, or services originating from any City account;
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
- Port scanning or security scanning is expressly prohibited unless prior authorisation has been granted by the Manager ICT;
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;
- Circumventing User authentication or security of any host, network or account;
- Introducing honeypots, honeynets, or similar technology on the City network;
- Interfering with or denying service to any User other than the employee's host (for example, denial of service attack);
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet;
- Use of unauthorised file sharing systems; and
- Providing information about, lists of, or photographs of employees to parties outside the City.

Internet

When using organisational resources to access and use the Internet, Users must realise they represent the City. Whenever employees state an affiliation to the City, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of the City”.

Reasonable Personal Use is permitted (see definitions). The City will, on occasions, monitor internet use to ensure Acceptable Use.

Acceptable Use of the internet involves:

- using it for business activities necessary to carry out job functions;
- communicating between City personnel and suppliers;
- getting CIS technical support to install software upgrades and patches;
- reviewing web sites for product information;
- referencing regulatory or other technical information; and
- carrying out research and other work related information searching which is relevant to job function.

Unacceptable Use of the Internet includes:

- accessing social networking sites without authorisation, e.g., Facebook, Twitter and MySpace;
- downloading music, movies or any software programs or files for use without authorisation;
- ordering (shopping) personal items or services on the Internet during core working hours;
- playing online games;
- participation in any on-line contest or promotion;
- accessing pornographic or sexually explicit web sites;
- acceptance of promotional gifts;
- streaming video or radio content unrelated to a job function;
- accessing material of an offensive, obscene, threatening, abusive or defamatory nature;
- using the internet for commercial activities not directly related to the City; and
- Users must exercise caution when choosing to click on ‘pop-up’ sites and/or adverts.

Email

Reasonable Personal Use is permitted although this should not impact on the delivery of the City’s services. Personal use should be restricted to before/after work and lunch breaks. All emails recording business communications are the City’s corporate records and must be registered into the City’s Electronic Content Management (ECM) system. They can be accessed only by authorised personnel.

Acceptable Use of email involves:

- using it primarily for work-related purposes;
- ensuring the content and distribution of emails respects confidentiality and privacy;
- ensuring distribution of email does not waive any legal professional privilege the City may be entitled to claim; and
- use of appropriate and respectful language and tone.

Unacceptable Use of email includes:

- sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam);
- creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type;
- any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages;
- unauthorised use, or forging of email header information;

- solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
- use of unsolicited email originating from within the City's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by the City or connected via its network;
- posting the same or similar non-business-related messages to large numbers of Usernet newsgroups (newsgroup spam);
- registering a work email address on any non-work related site e.g. Facebook or Twitter;
- distributing confidential or sensitive material via e-mail;
- use of email for commercial activities not directly related to the City;
- 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;
- emailing material which contains viruses, worms, 'Trojan horses' or any other contaminating or destructive features;
- charity requests, petitions for signatures, chain letters or letters relating to pyramid schemes and broadcasting messages;
- redirecting, forwarding, copying or moving email containing City business information to personal email addresses;
- social chatting with colleagues which is outside of Reasonable Personal Use.

Telecommunications

Acceptable Use must be made of telephones and mobile phones allocated to Users. These resources must be used for work-related purposes.

Acceptable Use of telephones, mobile phones and other mobile devices involves:

- using it primarily for work-related purposes;
- ensuring the content and distribution of SMSs and MMSs respects confidentiality and privacy;
- use of appropriate and respectful language and tone.

Unacceptable Use of telephones, mobile phones and other mobile devices includes:

- making calls that are offensive, obscene, threatening, abusive or defamatory;
- use of telephones and mobiles for commercial activities not directly related to the City;
- inappropriately transmitting information which may violate the rights of others, including unauthorised text, images or programs, trade secrets, confidential property or trademarks;
- Use of telecommunications equipment outside of Australia, unless prior approval has been granted by the CEO;
- Connecting City owned mobile computing devices to public Wi-Fi networks; and
- Use by family members, relatives or any external third party.

Reasonable Personal Use is permitted for communication within Australia only. The City will not pay for <u>any</u> personal international telecommunications (data or voice) usage and costs – these costs will be invoiced to the relevant User. Personal usage deemed by your Business Unit Manager or Director as beyond reasonable personal usage/cost (data and voice) will be invoiced to the relevant User.

All hardware including phones remains the property of the City. All hardware that is replaced, including telecommunications equipment, must be returned to CIS prior to receiving a replacement.

Mobile phones, iPads, Tablets and other mobile devices with access to the Internet and Email must also comply with the above sections relating to Acceptable Use of the Internet and Email. The City will not pay for <u>any</u> personal use that results in data plans, for any device, being exceeded – these costs will be invoiced to the relevant User. It is the responsibility of each User to monitor their data plan usage to avoid excessive costs being incurred.

Standards

Standards apply to the use of the City's IT Resources.

The following **email** standards apply:

- The external email naming standard is Firstname.Lastname@stirling.wa.gov.au;
- Users are not permitted to alter or remove the standard email signature block from emails when sending business related emails;
- Photographs of Users will be displayed on all internal emails and other internal systems;
- Users must remove the email signature block when sending personal emails;
- External email will have a standard disclaimer automatically appended;
- The maximum size email attachment is 10 megabytes; and
- During periods of absence from the office, the Outlook Out-of-Office Assistant auto reply must be activated advising non-availability and possible alternative contact options.

The following telecommunications standard applies:

- During periods of absence from the office, telephones are to be diverted to the appropriate alternative contact.

The following **password** and authentication standards apply:

- Passwords must have a minimum length of ten (10) characters and must contain at least three (3) of the following character sets:
    - Upper case (A-Z)
    - Lower case (a-z)
    - Digits (0-9); and
    - Special characters or punctuation e.g.$, %, #, @
    - For example –M0vE4bi!1Ty meets the corporate password standard.
- portable mobile computing devices such as iPads and iPhones will require six digit PIN;
- a User cannot change their password more than once a day;
- the password history will be set to a minimum of 12 previous passwords;
- where possible Multifactor authentication (MFA) must be used in conjunction with passwords. This includes and is not limited to the use of the Microsoft Authenticator App, or other multifactor authentication methods approved by the City;
- With the provision that user accounts have MFA enabled, the following standards apply:
    - a User's passwords must be changed every 180 days; and
    - a User's account will be locked out after three (3) unsuccessful login attempts within a 5-minute period; and
    - The user's account will be automatically unlocked after a period of fifteen (15) minutes.
- For user accounts that do not have MFA enabled, the following standards apply:
    - a User's passwords must be changed every 60 days; and
    - a User's account will be locked out after three (3) unsuccessful login attempts within a 5-minute period; and
    - the User's account will not be automatically unlocked;
    - to unlock their account, the user will need to either use the Self-Service Password Reset (SSPR) option or call the CIS Help Desk for assistance.
- where a password reset is required and the User has forgotten it or is unable to access their account, it is recommended that they use the SSPR option found in in the Microsoft Authenticator App to reset their password. Alternatively, if they do not have the Microsoft Authenticator App, they should call the CIS Help Desk for assistance. Security related information may be required to validate their identity as part of the password reset procedures;
- a User's session will be automatically locked if the session remains idle for more than 10 minutes.

Policy Compliance

The City reserves the right to verify compliance to this policy through various methods, including but not limited to monitoring usage, reviewing logs, accessing cookie history and engaging internal and external audits. Users acknowledge that their usage may be monitored.

Exceptions

Any exception to the policy must be approved by the CEO in advance.

Non-Compliance

Any User found to have violated this policy may be subject to the provisions set out in the Employee Discipline Management Practice.

Definitions

Chain letters - A typical **chain letter** consists of a message that attempts to convince the recipient to make a number of copies of the **letter** and then pass them on to as many recipients as possible.

CIS means the Corporate Information Services business unit.

Cookies is data stored on a local computing device which is used to collect identifying information about the User, such as Web surfing behaviour or User preferences for a specific Web site.

Denial of service - A **denial-of-service** attack is characterized by an explicit attempt by attackers to prevent legitimate Users of a **service** from using that **service.**

E-mail bombs - an **email bomb** is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox.

Encrypted - **encryption** is the process of encoding messages or information in such a way that only authorized parties can read it.

Forged routing – faking messages and rerouting them to an alternate destination.

Honeypots / honey nets – Honey Pots are fake computer systems, setup as a "decoy", that are used to collect data on intruders.

Host – any computer that has full two-way access to other computers on the internet e.g. a web server that serves pages for one or more Web sites.

Information and Technology Resources means the City's technology, information, email, internet, information systems and communication networks.

Internet – a term used to describe connecting multiple separate networks. Internet usage refers to accessing the internet either via a wired (Ethernet) or a wireless (Wi-Fi) network.

Intranet – A computer network based on internet technology that the organisation uses for its own internal purposes. E.g. SharePoint.

MFA – refers to Multi-Factor Authentication methods required for additional cyber security, such as the Microsoft Authenticator App.

Network sniffing - A **network sniffer** is a computer tool that captures network data.

Packet spoofing – spoofed or fake IP address.

Pinged floods - A **ping flood** is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP Echo Request (ping) packets.

Ponzi or other pyramid - A **Ponzi** scheme is a fraudulent investment operation where the operator, an individual or organisation, pays returns to its investors from new capital paid to the operators by new investors, rather than from profit earned by the operator.

Port scanning or security scanning - A **port scanner** is a software application designed to probe a server or host for open ports.

Reasonable Personal Use means the use of City of Stirling telephone, mobile devices, PC/Laptops and IT resources (including but not limited to internet and email), that does not negatively impact upon the Users work performance, hinder the work of others, involve modification of any IT resources, does not compromise or impact the security of the City's operations, expose the City to risk or negatively impact its reputation.

Trojan horses - A **Trojan** horse, or **Trojan**, in computing is a generally non-self-replicating type of malware program containing malicious code.

Users are employees, work experience personnel, volunteers, contractors, consultants, temporary and other category personnel who use the City information and technology resources (including Elected Members).

Virus - A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels.

Worms - Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

Relevant management practices/documents

City of Stirling Code of Conduct
Data Custodian Management Practice
Social Media Management Practice
Information Security Management Practice
Mobile Computing Device Management Practice
Employee Discipline Management Practice
Misconduct Control Management Practice
Misconduct Investigations 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**	10 May 2022	**Resolution #**	0522/011
Next review due	**Date**	2024		