Administration

Internet, Email Usage and Access to IT Systems Policy

Objective

This policy sets out the conditions for acceptable use of the Shire of Koorda's ("**the Shire's**") corporate information and communication technology (**ICT**) facilities. The Shire's ICT facilities include but are not limited to the Shire's network, computer systems, access to the internet and email, corporate systems and corporate hardware.

The purpose of this policy is to:

- regulate and provide guidelines on the proper use of the Shire's ICT facilities for their intended purposes without infringing legal requirements or creating unnecessary business risk, and
- protect against the risk of virus/malware attacks, theft and disclosure of information, and disruption of network systems and services.

Policy

Application

This policy applies to all employees, elected members, contractors, visitors and volunteers (collectively referred to as **authorised users** in this policy) engaged or appointed by the Shire while on the Shire's premises or while engaged in Shire related activities.

Definitions

TERM	DEFINITION
Authorised User	Any person that has been granted authorised access to the Shire's ICT facilities.
Email	The Shire provided Microsoft Outlook, Outlook Web Access, or any Shire email system that is synchronised to a PC or mobile device, whether the mobile device is provided by and remains the property of the Shire, or owned by an Authorised User.
ICT	Information, Communications, and Technology. This includes but is not limited to mail, telephones, mobile phones, voice mail, SMS, email, intranet, computers, tablets, printers, multi-functional devices, scanners and other electronic devices owned by the Shire
Malware	An abbreviation of 'malicious software' and means software programs designed to cause damage and other unwanted actions on a computer system. Examples of malware include spyware, worms, viruses and Trojans.
Network Access	Includes connectivity from any device to Shire managed ICT infrastructure connecting both local and remote network servers.
Prohibited Material	Content which: • could be reasonably regarded as pornographic; • contains offensive language, cruelty or violence; • is illegal, defamatory or discriminatory; • breaches copyright; • promotes terrorism or encourages terrorist acts; and • contravenes the Shire's values and policies.

General use of ICT equipment

Data created and stored on the corporate systems remain the property of the Shire. Because of the need to protect the Shire's network, the confidentiality of personal (non-work-related) information stored on any network device belonging to the Shire cannot be guaranteed.

For security and network maintenance purposes, authorised members of the Executive or the ICT Department within the Shire may monitor equipment, systems, network traffic and emails at any time, according to the specific nature and requirements of their roles.

The Shire reserves the right to audit networks and systems periodically to ensure system integrity and compliance with this policy.

Personal use

A degree of reasonable personal use of the Shire's ICT assets is allowed on the Shire's equipment/devices/systems.

Employees should exercise conservative judgment regarding the reasonableness of personal use and be guided by the following principles:

- Personal use should be undertaken either before or after contracted hours of work or during authorised breaks.
- Personal use should be limited and brief, avoiding excessive download or transmission. An example of acceptable personal use would be conducting brief transactions through internet banking.
- If there is any uncertainty regarding acceptable personal use then employees should consult their supervisor or line manager for guidance.

Security and proprietary information

All information stored on the Shire's corporate systems should be regarded as confidential and care must be exercised before sharing or distributing any information. If there is any uncertainty regarding the level of confidentiality involved then employees should consult their line manager for guidance.

Passwords and accounts must be kept secure and must not be shared. Authorised Users are responsible for the security of their passwords and accounts. Passwords should be changed in accordance with advice from the ICT team.

All devices connected to the Shire's computing systems/networks, regardless of ownership, must be running approved and up to date virus-scanning software. Employees must be attentive to emails they receive from outside parties and use caution when opening files received from unknown senders. The IT manager must be advised of any warning received by employees to determine if it is appropriate to advise all staff of the warning.

Email and communication activities

All emails sent by Authorised Users should include the 'signature' and disclaimer at the foot of the body of the email, in the format specified by the Shire's style guide or as otherwise advised by the Deputy Chief Executive Officer.

The following activities are not permitted when using a Shire email address:

- except in the course of normal business notifications, sending or forwarding unsolicited electronic messages, including the sending of 'junk mail' or other advertising material, jokes, or chain communication to individuals who did not specifically request such material,
- any form of harassment via electronic/ICT means,
- use of any of the Shire's network or systems for the purpose of generating unsolicited communications,
- sending any confidential Shire information to parties outside Shire or to personal email addresses,

- communicating in a manner that could adversely affect the reputation or public image of the Shire, and
- communicating in a manner that could be construed as making statements or representations on behalf of the Shire without the Shire's express permission to do so.

The use of personal email accounts (e.g. Gmail, Hotmail, Yahoo Mail, etc.) is not permitted for the conduct of Shire business.

Remote access

Users with remote access are reminded that when connected to the Shire's network, their devices are an extension of that network and as such are subject to the same rules and regulations that apply to the Shire's corporate equipment and systems.

The device that is connected remotely to the Shire's corporate network must be secure from access by external non-Shire parties and should be under the complete control of the user.

All devices (whether personal or corporate) connected to the Shire's networks via remote access technologies should have up-to-date anti-Malware software.

Where possible, users should avoid using public access terminals to establish a remote connection.

Unacceptable use

Under no circumstances is any user authorised to engage in any activity that is illegal under Local, State, Federal or International law while connected to or utilising Shire ICT systems or resources.

a) Prohibited material

Employees must not distribute emails, phone messages or documents (electronic or otherwise) under any circumstances that include information or activities which relate to Prohibited Material.

b) System and network activities

The following activities are not permitted:

- Violations of the rights of any person or company/organisation protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the duplication, installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by the Shire or the end user.
- Unauthorised copying or digitising of copyrighted material and the installation of any copyrighted software for which the Shire or the end user does not have an active license.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Introduction of Malware or code into the network or onto devices connected to the network.
- Revealing your account password to others or allowing use of your account by others.
- The Shire's equipment is not be used to download or distribute any material that could be considered offensive or Prohibited Material. If a user receives such material they should notify their line manager.
- Making fraudulent offers of products, items, or services, or undertaking private work via any Shire equipment, device or account.

The following activities are not permitted unless they are within the scope of regular responsibilities for an expressly authorised role:

- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access.
- Executing any form of network monitoring which will intercept data not intended for the user's host.
- Attempting to avoid or bypass the Shire's network security measures.
- Interfering with any other user's account, by whatever means.
- Using the system in a way that could damage or affect the performance of the network.

Provision and use of mobile phones and electronic devices

Some employees may be provided with a mobile phone, tablet and/or other electronic devices if it is deemed necessary to their position. All electronic devices supplied remain the property of the Shire and users of these devices must comply with this policy.

Consequences of breaching this policy

This policy constitutes a lawful instruction to employees. Any breach of this policy may lead to disciplinary action including, but not limited to, termination of employment.

In addition to disciplinary action, the Shire reserves the right to temporarily block or remove email, internet and Network Access for employees in breach of this policy.

Variation to this policy

This policy may be cancelled or varied from time to time. The Shire's employees will be notified of any variation to this procedure by the normal correspondence method.

Related Documents (Legislation/Local Law/Policy/Procedure/Delegation)

Code of Conduct
Disciplinary Policy
Social Media Policy

Review History

Review Due: March 2024

Date	Council Resolution	Description of review/amendment
28/06/2023	RES: 120623	V1.0. Re-write and merge old policies (A45 & A46) as per WALGA template.
Former Policy No: A45 E-mail Use & A46 Internet and WI-FI/LAN Use		
16/10/2013	RES: 051013	Adoption of Policy (A46)
16/10/2013	RES: 151013	Adoption of Policy (A45)