POLICY – 3.6 – Information Technology – Access and Use

Relevant Delegation
N/A

1. Objective

This Policy deals with the provision of information technology resources by the Shire and the associated responsibilities of authorised users when accessing these resources.

2. Policy Statement

This Policy outlines the conditions governing use of all IT (Information Technology) facilities provided by the Shire of Menzies.

Information technology resources are provided to support the Shires administrative and operation activities. These resources include the Shires network, desktop, computer systems and software, internet access, electronic mail (email), mobile devices and related services.

Users of these systems are expected to comply with the following Policy Schedule which is written with the intent of protecting the integrity of these systems so as to provide reliable IT services to users, and also to protect the right of each Elected Member and employee to work in a healthy and safe environment.

2.1. The following Schedule/s are adopted, and form part of this Statement –

- Policy Schedule 3.6 (a) – Principles of Access and Use of Information Technology
- Policy Schedule 3.6 (b) – Control, Management and Security
- Policy Schedule 3.6 (c) – Internet Access
- Policy Schedule 3.6 (d) – Email Use
- Policy Schedule 3.6 (e) – Internet and Email Record Keeping

– End of Policy

COMMENT

Refer to Schedule 3.6(a) – Principles of Access and Use of Information Technology – attached to this Policy

Formerly		
Last Reviewed	28 October 2021	
Next Review Date	February 2023	
Amended		
Adopted	29 November 2012 30 August 2018	25 June 2015 28 October 2021
Version	3	

Policy Schedule 3.6 (a) – Principles of Access and Use of Information Technology

1. Introduction

Information technology resources are provided to support the Shire's administrative and operational activities. These resources include the Shire's network (desktop, notebook and tablet computer systems and mobile phones) and software, internet access, electronic mail (email) and related services.

Users of these systems are expected to comply with the policy which is intended to protect–

- the integrity of these systems so as to provide reliable IT services to users, and
- the right of each Elected Member and employee to work in a healthy and safe environment.

2. Ethics

Respect the rights of others, and comply with other policies regarding occupational health and safety, harassment, equal opportunity etc. Do not engage in behaviour, which violates these policies.

Personal use must not interfere with or detract from work purposes, activity or employee time.

3. Legislation

a) Occupational Safety and Health

Employees have a duty not to adversely affect their own or any other person's health and safety at work. Distribution of offensive material through the Shire's IT systems that may cause trauma or distress to other employees, or the use of these systems to bully or intimidate other employees may be construed as a breach of the Occupational Safety and Health legislation.

b) Equal Opportunity

The Equal Opportunity Act 1984 WA prohibits discrimination (on grounds including gender, race and religion etc) and sexual harassment. Examples of discrimination and harassment include but are not limited to the following–

- reference to a particular class of persons based on their race,
- sending of pornographic material to a fellow employee,
- annoyance of others, interference or attempt to modify or destroy their work or data,
- behaviour that may be construed as intimidating or bullying.

c) Freedom of Information

Computer records including internet usage and emails are subject to FOI obligations.

d) Copyright

Respect the legal copyright rules. Copyright provisions also relate to downloading of software and documents. Do not distribute or install software without first obtaining approval from the Chief Executive Officer. Always assume website content to be subject to copyright unless stated otherwise.

e) Council Policy

Council Policies and instructions issued by senior staff apply. These include–

- Equal Employment Opportunity
- Occupational Health and Safety
- Harassment and Grievances
- Records Keeping Plan

f) Records Management

Respect the need to maintain other internal systems. Use of internet and email is subject to the State Records Act, and the requirements of the Shire's Record Keeping Plan.

4. Defamation

A person defames another if they publish a statement or comment (written or verbal) which is likely to cause an ordinary, reasonable member of the community to think less of that other or to shun or avoid that other. Generally, any comments which disparage another person's business or professional acumen, suggest that a person may have committed a crime or refer in a disparaging way to a person's personal attributes would be considered to be seriously defamatory. Any person who is party to the publication of defamation may be liable for payment of substantial damages.

5. Personal Use

Reasonable personal use of Shire IT resources may be permitted (in the user's own time) provided that it does not –

- negatively impact upon the user's work performance, hinder the work of others nor make any modification to any IT resource,
- result in additional cost to the Shire.

Reasonable use in a particular circumstance will be a matter to be determined by the Chief Executive Officer.

6. Restrictions

Prohibited uses of Shire IT resources are –

- any illegal purpose,
- transmission or access to any material in violation of any Commonwealth or State legislation, including copyright material, threatening or obscene material, or information protected by trade secret.
- conduct private commercial activities including eBay and similar online auction sites.
- access, create, store or distribute pornographic material of any type.
- to gamble or play games.

Users found to have breached this policy may be subject to disciplinary action under law or adopted Council policies.

Criminal offences will be reported to the Police. Penalties that may result can be substantial, e.g. up to $10,000 under the Occupational Health and Safety Act for some offences.

7. Mobile communications

In so far as is applicable, this policy applies to mobile phones, tablets etc provided for Shire purposes.

– End of Schedule

Policy Schedule 3.6 (b) – Control, Management and Security

1. Access Control

a) On-site and remote access to information systems is controlled by the Chief Executive Officer. Users are granted access on the basis that their use of IT resources shall be responsible, ethical and lawful at all times.
b) When a new employee commences, the Chief Executive Officer is to determine the level of system access required.
c) The Shire may modify, upgrade, withdraw or otherwise alter any IT facilities without notice.
d) The Shire has ownership of all files and e-mail messages stored on Shire computers and may examine and/or monitor without notice, all computer data and software on its facilities.

2. Computer Systems

a) Work Purpose – Computer systems are provided as a tool to support the operations of the Shire. Each computer is installed with a standard operating environment plus additional user specific tools.
b) Personal Use – Limited personal use of computer systems is allowed provided such use is reasonable in terms of time and cost.
c) Prohibited Use – Under no circumstance are users to install –
   - software or utilities on Shire computers that are not licensed, and work related. Permission must be obtained from the Chief Executive Officer before installing applications on Shire computers.
   - software or utilities sourced from the internet. This includes but not limited to ICQ, Gator, Neopets, Bonzibuddy, Internet flowers, Web shots and other screensavers.
   - any software on Shire computers without the prior permission of the Chief Executive Officer.
d) Monitoring – The Shire reserves the right to monitor email, internet activity, logs and any electronic files for any reason, including but not limited to, suspected breaches by the user of their duties, Council policy, or unlawful activities.
e) Maintenance of hardware and software – Maintenance of the Shire's IT systems is the responsibility of the Chief Executive Officer. Under no circumstance should any Elected Member or employee attempt to repair hardware or software faults without the permission of the Chief Executive Officer or by their instruction.

3. Security

a) Where the use of any IT facility is governed by a password, the password must not be inappropriately divulged to any other person, but precaution taken to ensure that their passwords, accounts, software and data are adequately protected.
b) Passwords should contain at least 8 characters and a mix of upper and lowercase alpha, and numbers.
c) Any computer account or facility allocated to a user is for their exclusive use. The user must not allow another person to use it without appropriate authorisation from the Chief Executive Officer.
d) Regardless of the prevailing security, users shall not access any data or software except data or software that belongs to the user or has been provided for their use or is stored on a shared medium for which they have been granted access.
e) Users must not attempt to rename, delete, or modify the data of another user without prior authorisation from the Chief Executive Officer, except in the following circumstances –
   - data or files stored on a shared network facility or transferred in/out via a shared network facility.

- under direction of their supervising officer(s) to amend data or files stored in a personal directory.

f) Anti-virus software protection is provided at both server and desktop level. If a user suspects that their machine has become infected with a virus it should be reported immediately to the Chief Executive Officer.

g) Users should correctly shut their computer systems down before finishing work each day, unless otherwise requested by the Chief Executive Officer.

h) Users must report to the Chief Executive Officer, without delay, any breaches (either real or perceived) of security.

– End of Schedule

Policy Schedule 3.6 (c) – Internet Access

1. Internet provision

Internet costs are incurred based upon the amount of data that is received from the internet and can be significant. The internet also presents a security risk to the Shire's operations. The following points are aimed at reducing the cost and risk of providing internet access.

It should be noted that downloading does not mean only copying a file or document over the internet to a computer – it is **all** information coming into the system from another computer, even if only viewed. The Shire is charged for all data received.

2. Internet Use

a) Work Purpose
Users are permitted to access the internet for work related purposes as outlined in each user's internet usage application.

b) Personal Use
Limited personal use of internet facilities is allowed, such as online banking, travel bookings, browsing, provided such use is reasonable in terms of time and cost.

c) Prohibited Uses
Use of internet must comply with the Principles outlined in Schedule 3.6 (a). Specifically prohibited is –

- streaming voice and video media unless work related – e.g.: on-line radio
- online games.
- use of chat rooms/channels or instant messaging applications,
- subscription services, unless approved by the Chief Executive Officer.
- use MP3 or MP4 download sites (predominantly music and movies),
- interfering or disrupting to any network, information service, equipment or any user,
- causing any person to view content which could expose the Shire to prosecution.

d) User responsibility
It is the user's responsibility to ensure that any internet site they access is within the bounds of acceptable and appropriate usage, legal and does not pose a risk to the security of the Shire's operations.

Web based applications must be approved by the Chief Executive Officer and the Chief Executive Officer informed of the intended use of the application so that appropriate security measures are taken.

– End of Schedule

Policy Schedule 3.6 (d) – Email Use

1. Legal Obligations

Users should be aware that email from the Shire is the same as a letter printed on Shire letterhead, and is therefore subject to the same legal, privacy and records management obligations as paper records and letters.

2. Email Facilities

a) Work Purpose
Email is provided to allow electronic communication with the Shire's partners, clients and staff.

b) Personal Use
Limited personal use is allowed provided such use is reasonable in terms of time and cost and does not interfere with Shire business or present a security risk.

c) Prohibited Uses
Use of email must comply with the Principles outlined in Schedule 3.6 (a), and in addition, specifically prohibited is –

- circulate personal contact information of employees of the Shire without their consent;
- disseminate any information that is confidential to Shire;
- subscribe to any subscription service, unless approved by the Chief Executive Officer.
- send forged messages.
- use someone else's mail address without authorisation.
- send aggressive, rude or defamatory messages.
- send unsolicited emails (SPAM) or distribute junk emails
- broadcast messages, regardless of interest, with the exception of urgent messages

d) User Responsibilities Users are required to –

- protect their email address as able to avoid inclusion in mass mailing lists (SPAM).
- correspondence via email should be of the same standard for written communication.
- report emails which contains anything controversial, offensive or discriminatory, to the Chief Executive Officer.
- treat email attachments with caution due to their susceptibility to viruses, malware etc. Discretion must be exercised, particularly where the email is from an unknown source.
- maintain compliance with any records procedures regarding email.

3. Email Accounts

a) Shire emails accounts (name@menzies.wa.gov.au) may only be created by the Chief Executive Officer.

b) Elected Members and employees are not to use private email accounts to conduct business associated with the role and purpose of Council. Elected Members and Employees who receive an inquiry from a community member, contractor, developer or other agency via their personal email should immediately direct the sender to forward that inquiry to their official Shire of Menzies address.

c) users should check their e-mail frequently, respond, or archive messages, delete any ephemeral messages promptly and manage their e-mail files wisely.

d) When absent for an extended period (training, conferences, leave etc), users should utilise the ability of the email software to –

- forward incoming mail to the person acting in/for the position during

their absence, or

- create an automated message advising of absence, and the appropriate contact person.

4. Email Disclaimer to be used

When an email is sent having a Shire logo or email address a suitable disclaimer is to be used, such as –

This e-mail message, including any attached files, is private and may contain information that is confidential. Only the intended recipient may access or use it. If you are not the intended recipient, please delete this e-mail and notify the sender promptly. The views of this sender may not represent those of the Shire of Menzies. The Shire uses virus- scanning software but exclude all liability for viruses or similar defects in any attachment.

– End of Schedule

Policy Schedule 3.6 (e) – Internet and Email Record Keeping

1. Shire of Menzies Record Keeping Plan

a) The principles and procedures of the Shire's Records Keeping Plan apply to documents downloaded from the internet, or received / sent as emails.
b) All corporate information including correspondence, minutes of meetings, memos, file notes and reports (other than those generated through the Shire's databases) are to be stored in the shared server . This is consistent with the legislative requirements of the State Records Act 2000.
c) E-mails and faxes, sent and received, of a corporate nature must be captured and stored in the shared server. This is consistent with the legislative requirements of the State Records Act 2000.
d) Corporate documents must not be stored on desktop computers or on portable media (e.g. thumb drives, CD's). There are appropriate methods for storing draft and 'working' documents within the shared server. Network drives are provided for non-corporate documents only and only limited quotas are allowed.
e) Only the network drives and corporate systems are backed up. 'C' drives are not backed up and users will be responsible for any loss of data stored on this drive or on portable media.
f) Duplication of data is to be avoided. Any documents stored in the shared server should not be stored elsewhere unless access to the shared server is planned to be unavailable or the data is stored on media specifically designed for the purpose of backup.

2. Internet documents

Due to the dynamic nature of the internet, information at a particular date that may be subject to change and which will have relied on in decision making should be copied either by printing and filing or creating a PDF of the page referenced.

Where the information will not change, there is no need to print or retain an e-copy, but reference to the data should be made.

3. Emails received and sent

Since multiple emails may be required to finalise a matter, progressive exchanges do not need to be printed and filed. Once the matter is concluded, if it is a significant matter that a hard copy is considered appropriate, it may then be printed and filed, particularly if–

a) it documents the actions of the Shire in some way
b) plays a significant part in making a decision, or
c) is annotated or has major alterations made by the Shire in some way.

Due to the dynamic nature of the internet, information that may be subject to change which may be relied on at a particular date in decision making should be copied either by printing and filing, or creating a PDF of the final email, including exchange and any final attachments.

Emails considered to be day to day administrative or relating to the progression of a task do not require printing and filing, however the electronic copies of all emails sent and received relating to a matter must be electronically retained in compliance with the State Records Act.

Emails that are ephemeral may be deleted.

– *End of Schedule*