POLICY NO.	A.13
POLICY SUBJECT	Information Communication Technology Use Policy
ADOPTION DATE	25 January 2001
LAST REVIEW DATE	26 November 2020 (C.05/1120)

1. Overview

Effective security is a team effort involving the participation and support of every Shire employee who deals with information and/or information systems and devices.

The Shire of Bridgetown-Greenbushes' information and/or information systems and devices are a corporate resource and are to be used for corporate business as a vehicle for business to business and business to customer transactions. Personal usage should be kept to a minimum.

Every digital device user must understand this policy and carry out their use of digital devices in accordance with this policy. For the purposes of this policy the term "employee/s" shall extend to cover contractors, volunteers and any person performing work for or with the Shire in any capacity.

2. Objectives of Policy

2.1 To ensure that the Shire's investment in information and/or information systems and devices is used in the most productive and appropriate manner to the greatest possible benefit of the Shire of Bridgetown-Greenbushes.

2.2 To ensure that all the organisation's digital information is preserved and available as corporate knowledge.

2.3 To uphold the reputation of the Shire in all digital and information based transactions.

3. Use of Information and/or Information Systems and Devices

3.1 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 supervisor or manager for guidance.

Passwords should be kept secure and accounts must not be shared. Authorised users are responsible for the security of their passwords and accounts. Passwords should be changed regularly.

All devices connected to the Shire's computing systems/networks, regardless of ownership, must be running approved and up to date virus-scanning software.

People must use caution when opening files received from unknown senders.

All corporate information which is owned (created or received) by the organisation are records under the State records Act and may have any or all of the following attributes:

3.1.1 Information which is of administrative, legal, fiscal, evidential or historical value and is not recorded elsewhere on the public record.
3.1.2 Formal communication and/or a transaction between officers (for example – memorandum, report or submission) or between an officer and another party; or
3.1.3 It may document the rationale behind agency policy, decisions or directives.

3.2 Personal Use of ICT Equipment

While the Shire's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remain the property of the Shire. Because of the need to protect Shire's network, the confidentiality of personal (non-work-related) information stored on any network device belonging to Shire cannot be guaranteed.

A degree of personal use is allowed on the Shire's equipment/devices/systems. Employees should exercise conservative judgment regarding the reasonableness of personal use but should be guided by the following principles:

3.2.1 Personal use should be conducted either before or after contracted hours of work or authorised breaks;
3.2.2 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;
3.2.3 Personal use should not breach anything in this policy, particularly relating to the downloading of offensive or copyrighted materials;
3.2.4 Managers will determine the specific acceptable personal use for their respective business areas as this will differ according to the needs of each group; and
3.2.5 If there is any uncertainty regarding acceptable personal use then employees should consult their supervisor or manager for guidance.

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

The Shire reserves the right to audit networks and systems on a periodic basis to ensure system integrity and compliance with this policy.

3.3 System and Network Activities

The following activities are not permitted:
3.3.1 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.
3.3.2 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.
3.3.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The CEO or appropriate Executive Manager should be consulted prior to export of any material where status is in unclear;

3.3.4 Introduction of malicious programs or code into the network or onto devices connected to the network;

3.3.5 Revealing an account password to others or allowing use of an employee's account by others.

3.3.6 The Shire's equipment is not be used for the downloading or distribution of any material that could be considered as offensive. If a user receives such material they should notify their manager.

3.3.7 Making fraudulent offers of products, items, or services, or running private business interests via any Shire equipment, device or account.

3.3.8 Undertaking private work.

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

3.3.9 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;

3.3.10 Executing any form of network monitoring which will intercept data not intended for the user's host;

3.3.11 Attempting to avoid or bypass Shire's network security measures;

3.3.12 Interfering with any other user's account, by whatever means; and

3.3.13 Using the system in a way that could damage or affect the performance of the network in any way.

3.4 Email and Communication Activities

3.4.1 All corporate emails sent or received via the Shire's email are the property of the Shire of Bridgetown-Greenbushes and thus form part of the organisation's record keeping system.

3.4.2 All corporate emails (incoming and outgoing) are to be downloaded and registered through the Inward/Outward Mail registers including appropriate File Numbers allocated by the receiver/author.

3.4.3 Attachments should not be opened or stored unless the employee can positively identify the sender. This is to ensure no virus is released into the Shire's computer system.

The following activities are not permitted:

3.4.4 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;

3.4.5 Any form of harassment via electronic/ICT means;

3.4.6 Unauthorised use, or forging, of email header information;

3.4.7 Send or distribute emails containing pornographic or derogatory content.

3.4.8 Any employee receiving questionable material (as outlined in3.4.7) should immediately report the incident to their supervisor for appropriate action.

3.4.9 Creating or forwarding "chain letters" or "pyramid" schemes of any type;

3.4.10 Use of any of the Shire's network or systems for the purpose of generating unsolicited communications;

3.4.11 All staff and Elected Members are required to protect the confidentiality provisions of the Shire, exercise due care and adhere to confidentiality agreements when handling data or information on/from the Shire's computer

system. This includes providing information about, or lists of the Shire's employees to parties outside the organization or to personal email addresses;

3.4.12 Communicate in a manner that could adversely affect the reputation or public image of the Shire; and

3.4.13 Communicate 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.

3.5 Remote Access

Users with remote access should be reminded that, when they are connected to the Shire's network, their machines 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. That is, their machines need to connect and communicate reliably with the Shire's network and servers to ensure the security and integrity of data and records.

Users are reminded of the following conditions relating to remote access to the Shire's system:

3.5.1 Family members must not violate any of the Shire's policies, perform illegal activities, or use the access for outside business interests;

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

3.5.3 The use of non-Shire email accounts (e.g. Yahoo, Hotmail, Gmail etc.) or other external resources is not permitted for the conduct of Shire business, thereby ensuring official business is not confused with personal business; and

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

3.6 Provision and Use of Mobile Phones and Information/ Communication Devices

Some employees will be supplied with a mobile phone and/or other mobile computing devices if it is deemed necessary to their position. All mobile/portable devices supplied remain the property of the Shire and users must not change service providers unless permitted to do so.

Where a mobile phone or device provides an email service, all emails sent or received or otherwise processed via the mobile device that are classified as a record of the Shire should be through the Shire's server, to ensure the integrity of the recordkeeping system.

Where the device includes a digital camera, users are to operate the technology in a sensible manner. A failure to do so may lead to disciplinary action including possible termination of employment. Employees may also be held criminally liable for their actions.

It is unlawful for drivers to operate a mobile phone and/or other mobile computing device whilst driving. Phone calls may otherwise be made or received providing the device is accessible while mounted/fixed to the vehicle or does not need to be touched by the user. An employee who operates a mobile phone and/or other mobile computing device whilst driving may face disciplinary action including possible termination of employment. Employees may also be held criminally liable for their actions.

Consequences of Breaching this Policy

Any employee or elected member found to have breached this policy may be subject to disciplinary action including possible termination of employment. The Shire may also be obligated to refer any breach of this policy to an external agency where an employee may be held criminally liable for their actions.

Private/personal or unauthorised use of corporate ICT systems and/or devices may result in the user being obligated to pay any extra costs incurred. The CEO will determine breaches for staff the Council will determine breaches for the CEO and Elected Members.