Administrative Policies - 2.9 Information and Communication Technology (ICT) Use Policy

Policy	Administrative Policies - 2.9 Information and Communication Technology (ICT) Use Policy
Purpose	To ensure effective security is maintained by every employee who deals with information and/or information systems and devices.
Status	Administrative - Statutory

Policy

General 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 the Shire's network, the confidentiality of personal (non-work-related) information stored on any network device belonging to the Shire cannot be guaranteed; and
- A degree of personal use is allowed on Shire's equipment/devices/systems. Employees should exercise conservative judgement regarding the reasonableness of personal use but should be guided by the following principles:
    - Personal use should be conducted either before or after contracted hours of work or authorized 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;
- Personal use should not breach anything in the policy, particularly relating to the downloading of offensive or copyrighted materials;
- 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
- 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, authorized 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.

All emails sent by Shire staff 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 CEO.

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 in accordance with the Shire's advice from the ICT consultant.
- All devices connect to the Shire's computing systems/networks, regardless of ownership, must be running approved and up to date virus-scanning software; and

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

Unacceptable Use

The information in this policy provides a framework for activities which fall into the category of unacceptable use, but do not represent an exhaustive list. Some users are exempted from these restrictions during the course of carrying out responsibilities related to their role. 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 the Shire's ICT systems or resources.

Systems 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. The appropriate manager should be consulted prior to export of any material where status is in unclear;
- Introduction of malicious programs 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 to 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 and also the ICT Team;

- Making fraudulent offers of products, items, or services, or running private business interests via any Shire equipment, device or account; and
- Undertaking private work.

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

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

Email and Communications Activities

The following activities are not permitted:

- 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;
- Unauthorised use, or forging, of email header information;
- Solicitation of communication for any other electronic address, other than that of the poster's account, with the intent to harass or to collect replies;
- Creating or forwarding "chain letters" or "pyramid" schemes of any type;

- Use of any of the Shire's network or systems for the purpose of generating unsolicited communications;
- Providing information about, or lists of the Shire's employees to parties outside the 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 express permission to do so.

Users should also endeavour to clean out their Inbox, Sent Items, Deleted Items and other email boxes on a regular basis, by either deletion or saving in the central record system. A size limit per mailbox may be implemented to ensure that the system is functioning optimally.

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:

- Family members must not violate any of the Shire's policies, perform illegal activities, or use the access for outside business interests;
- 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;
- The use of non-Shire email accounts (e.g., Yahoo, Hotmail, Gmail etc.) or other external resources is not permitted for the conduct of Council business, thereby ensuring official business is not confused with personal business; and
- 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.

Provision and use of Mobile Phones and Information/communication Devices

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

Where a mobile 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 use 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 theiractions.

Consequences of Breaching This Policy

- Any user 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.

Variation to This Policy

This policy may be cancelled or varied from time to time. All the Shire's employees will be notified of any variation to this policy by the normal correspondence method. All users of the organisations ICT are responsible for reading this policy prior to accessing the organisations ICT.

Related Procedure	Code of Conduct Social Media Use Policy
Amended Authority Level	Council
Related Local Law/Legislation	
Adopted/Amended	December 2016