Administration 7 – SHIRE OF CHRISTMAS ISLAND INFORMATION COMMUNICATIONS TECHNOLOGY (ICT) USE POLICY

1. Policy Statement

1.1. Effective security is a team effort involving the participation and support of every Shire of Christmas Island employee who deals with information and/or information systems and devices. Every digital device user must understand this policy and carry out their use of digital devices in accordance with this policy.

1.2. 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 of Christmas Island in any capacity. All employees with access to Shire ICT workstations or equipment will be required to sign the Statement of Understanding and receipt of the ICT Use Policy.

2. General Use of ICT Equipment

2.1 While Shire of Christmas Island'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 Shire of Christmas Island. Because of the need to protect Shire of Christmas Island's network, the confidentiality of personal (non-work-related) information stored on any network device belonging to Shire of Christmas Island cannot be guaranteed.

2.2 A degree of personal use is allowed on the Shire of Christmas Island's equipment/devices/systems. Employees should exercise conservative judgment 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 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;
- Personal use should not breach anything in this 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.

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

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

2.5 All emails sent by Shire of Christmas Island staff should include the 'signature' and disclaimer at the foot of the body of the email, in the format specified by the Shire of Christmas Island's style guide or as otherwise advised by the Director of Governance

3. Security and Proprietary Information

3.1 All information stored on the Shire of Christmas Island'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;

3.2 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 AD 10 – Network Security Management Policy.

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

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

4.0 Unacceptable Use

4.1 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.

4.2 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 of Christmas Island ICT systems or resources.

5.0 System and Network Activities

5.1 The following activities are not permitted:

a) 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 of Christmas Island or the end user;

b) Unauthorised copying or digitising of copyrighted material and the installation of any copyrighted software for which the Shire of Christmas Island or the end user does not have an active license;

c) 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;

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

e) Revealing your account password to others or allowing use of your account by others;

f) The Shire of Christmas Island'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 and also the ICT Team;

g) Making fraudulent offers of products, items, or services, or running private business interests via any Shire of Christmas Island equipment, device or account; and

h) Undertaking private work on SOCI ICT equipment or network, including using personal devices with SOCI wifi access; and

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

6.0 Email and Communications Activities

(a) The following activities are not permitted:

(b) 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;

(c) Any form of harassment via electronic/ICT means;

(d) Unauthorised use, or forging, of email header information;

(e) 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;

(f) Creating or forwarding "chain letters" or "pyramid" schemes of any type;

(g) Use of any of the Shire of Christmas Island 's network or systems for the purpose of generating unsolicited communications;

(h) Providing information about, or lists of the Shire of Christmas Island 's employees to parties outside Shire of Christmas Island or to personal email addresses;

(i) Communicating in a manner that could adversely affect the reputation or public image of Shire of Christmas Island; and

(j) Communicating in a manner that could be construed as making statements or representations on behalf of Shire of Christmas Island without the Shire of Christmas Island 's express permission to do so.

6.2 Users should also endeavor 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.

The ICT Officer is to assist staff in managing the back-up of Outlook mailboxes if requested.

7.0 Remote Access

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

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

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

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

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

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

8.0. Provision and Use of Mobile Phones and Information/ Communication Devices

8.1 Some people will be supplied with a laptop/ mobile phone and/or other mobile computing device if it is deemed necessary to their position. All devices supplied remain the property of the Shire of Christmas Island**.**

8.2 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.

8.3 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.

9.0. Consequences of Breaching This Policy

9.1 Any user found to have breached this policy may be subject to disciplinary action including possible termination of employment. The Shire of Christmas Island 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.

9.2 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.

Document Control Box

Version	Approved, Amended, Rescinded	Date	Officer	Resolution number	Key changes/ notes	Next Review date	File Ref No.
1	Approved	21/3/2023	Chirs Su	15/23			