

Purpose

To provide guidelines for the acceptable use of Council Information and Communications Technology (ICT) assets by Council Members, employees, contractors and volunteers.

Background and Issues

Acceptable use of the Shire of Northampton's (Shire) information and communication technology resources will underpin the organisation's ability to keep pace, grow and innovate whilst maintaining increased and affordable access to and protection of data and services. Acceptable use of ICT resources and services creates a secure, well managed and more efficient workplace.

Objectives

To support the safe and effective use of Council ICT assets by:

- Controlling risks associated with cyber security threats to Council ICT assets;
- Protecting the privacy of personal information; and
- Preventing inappropriate and unlawful use of ICT assets.

Area of Application

This policy applies to Council Members, Council Employees, ICT providers to Council, Contractors, Volunteers and any other person who is provided access to Council ICT assets.

Policy Measures***1. Business Purposes***

The Shire of Northampton's (Shire) ICT systems and resources are tools to be used for Shire business purposes.

Use of the Shire of Northampton's ICT systems must:

- a) Be for Shire business purposes only, or where authorised or required by law, or with the express permission of an Authorised Person; and
- b) Be used like other business communications and comply with any code of conduct or legislative requirements that apply to the user.

Notwithstanding clause 1(a), users of the Shire of Northampton's ICT systems may use those systems for personal use provided the use is minor and infrequent and does not breach this Policy.

Users must not engage:

- a) In excessive personal use of the Shire's ICT systems during working hours; or
- b) In excessive personal use of electronic communications and the internet using Shire's networks outside working hours.

A breach of either of these constitutes a failure to abide by this Policy.

Minor and infrequent personal use must be conducted as follows: in accordance with this clause:

- a) Subscribing to list servers, mailing lists and other similar services must be for Shire purposes or professional development reasons only; and
- b) Online conferences, discussion groups or other similar services must be relevant and used for Shire purposes or professional development activities. Such interaction requires that internet etiquette should be observed along with current societal standards for respect and fairness.

Obtaining unauthorised access to electronic files of others or to email or other electronic communications of others, is not permitted and may constitute a criminal offence.

Large downloads or transmissions should be minimised to ensure the performance of the Shire's ICT systems for other users is not adversely affected. Where a user has caused the Shire to incur costs for excessive downloading of non-work related material in breach of this policy, the Shire may seek reimbursement or compensation from the user for all or part of these costs or apply other forms of disciplinary action.

2. Shire Property

The Shire of Northampton is the owner of, and asserts copyright over;

- a) All electronic communications created by employees as part of their employment and traverse with the Shire's ICT systems.
- b) All electronic data / information stored on the Shire's ICT systems.
- c) Personal devices if they are fitted with Shire software

Electronic communications created, sent or received by the users referred to in the 'Area of Application' of this Policy are the property of the Shire, and may be accessed as records of evidence in the case of an investigation. All electronic communications are kept for 7 years. Electronic communications may also be subject to discovery in litigation and criminal investigations. Please note that email messages and mobile phone text messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent. This clause is subject to Commonwealth or State law that precludes such access.

3. Monitoring

Use of the Shire's ICT systems may be monitored by Authorised Persons.

Shire employees shall have no expectation of privacy in anything they store, send or receive on the Shire's information systems. The Shire may monitor messages without prior notice. The Shire is not obliged to monitor email messages.

From time to time, Authorised Persons may examine or monitor the records of Shire's ICT systems including for operational, maintenance, compliance,

(ICT) System Acceptable Use

auditing, security or investigative purposes. For example, electronic communications and web sites visited may be monitored. The Shire of Northampton may investigate a complaint arising from the use of the Shire's ICT systems.

Use of the Shire's ICT systems is provided to users on condition that it is agreed that the Shire's ICT systems are monitored in accordance with this Policy. Use of the Shire's ICT systems constitutes consent to monitoring in accordance with this Policy.

If at any time there is a reasonable belief that the Shire's ICT systems are being used in breach of this Policy, the CEO or the Manager of the person who is suspected of using the Shire's ICT systems inappropriately may suspend all or any part of a person's use of the Shire's ICT systems and may require that the equipment being used by the person be secured by the CEO or the manager while the suspected breach is being investigated.

4. Defamation

Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread. The Shire's ICT systems must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or Shire of Northampton liability.

5. Copyright Infringement

The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or the Shire of Northampton liability, despite the belief that the use of such material was permitted.

The Shire of Northampton supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement. Copyrighted material will be deleted if discovered.

6. Illegal Material

The Shire's ICT systems must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and will be viewed as a serious breach of the terms of employment and appropriate action taken.

Illegal or unlawful use includes but is not limited to use of certain types of

pornography (e.g. child pornography), defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking, use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under various Crimes Acts or any other relevant legislation.

7. *Offensive or Inappropriate Material*

Use of the Shire's ICT systems must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

The Shire's ICT systems must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually oriented messages or images and messages that could constitute sexual harassment (sometimes referred to as flaming).

All users of the Shire's ICT systems should be familiar with any Shire of Northampton anti-discrimination, equal opportunity and harassment policies.

Users of the ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their Manager. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto the Shire's ICT systems except where the material is required for the purposes of investigating a breach of this policy.

8. *Confidentiality*

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of the Shire's ICT systems, users must be aware that this security is not guaranteed, particularly when communicating to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

9. *Malicious Software*

Electronic communications are potential delivery systems for various forms of computer viruses. All data, programs and files which are downloaded electronically or attached to messages or imported on any other media (e.g. thumb drives, flashcards, iPods, removable disks, cameras) should be scanned by an anti-virus program before being launched, opened or accessed.

Viruses have the potential to seriously damage the Shire's ICT systems. Do not open any downloaded files, emails or attachments that you are not expecting or that look suspicious. If you receive any files that you suspect contain a virus it should be reported immediately to the ICT Department.

10. Attribution

There is always a risk of false attribution of breaches of this Policy. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances, an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, the ICT Department should be informed.

Users are accountable for all use of Shire's ICT systems that have been made available to them for work purposes and all use of the Shire's ICT systems performed with their user-ID. Users must maintain full supervision and physical control of the Shire's ICT equipment, including notebook computers and mobile phones at all times. User-IDs and passwords must be kept secure and confidential. User-IDs and passwords should not be disclosed to anyone, including disclosure to Managers or Senior Management. Users must not allow or facilitate unauthorised access to the Shire's ICT systems through the disclosure or sharing of passwords or other information designed for security purposes.

Active connections are to be terminated when access is no longer required and personal computers and devices secured by password when not in use.

11. Mass Distribution and "Spam"

The use of electronic communications for sending junk mail, for-profit messages, or chain letters is strictly prohibited. Mass electronic communications should only be sent in accordance with normal Shire of Northampton procedures.

The use of electronic communications for sending unsolicited commercial electronic messages ('Spam') is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

12. Records Management

Electronic communications are public records and subject to the provisions of the *State Records Act 2000*.

Shire of Northampton record management practices for management of email messages must comply with Shire policies and guidelines on recordkeeping and management of electronic communications as amended from time to time. Email messages that are routine or of a short-term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records.

Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be

maintained in a user's mailbox.

13. Email Disclaimer

All emails sent externally from the Shire of Northampton will have a disclaimer placed along with the employee's signature. The current disclaimer is worded as follows:

"This e-mail and any attachment(s), is confidential and may be legally privileged. It is intended solely for the recipient(s). If you are not the recipient, dissemination, copying or use of this e-mail or any of its content is prohibited and may be unlawful. If you are not the intended recipient please inform the sender immediately and destroy the e-mail, any attachment(s) and any copies. All liability for viruses is excluded to the fullest extent permitted by law. It is your responsibility to scan or otherwise check this email and any attachment(s). Unless otherwise stated (i) views expressed in this message are those of the individual sender, except where the message states otherwise and the sender is authorised to state those views on behalf of the Shire of Northampton (ii) no contract may be construed by this e-mail. Emails may be monitored and you are taken to have consented to this monitoring."

This disclaimer must not be altered or interfered with in any way, except by the Manager of Corporate Services with approval of the CEO. The use of this disclaimer may not necessarily prevent the Shire of Northampton or the sender of the email from being held liable for its contents.

14. Complaints

If a Shire officer wishes to make a complaint about an electronic communication that is offensive or inappropriate, raise it with the Manager of Corporate Services or the officers direct Manager.

15. Non-Compliance

Depending on the nature of the inappropriate use of the Shire's ICT systems, non-compliance with this Policy may constitute:

- a) A breach of employment obligations;
- b) Serious misconduct;
- c) Sexual harassment;
- d) A criminal offence;
- e) A threat to the security of the Shire of Northampton's ICT systems;
- f) An infringement of the privacy of staff and other persons; or
- g) Exposure to legal liability.

Non-compliance with this Policy will be regarded as a serious matter and appropriate action may be taken.

16. Breaches of this Policy

Breaches of this Policy may be classified using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. Matters not covered by the following categories will be dealt with on an individual basis and by consideration of the relevant facts.

Category 1: Illegal

This category covers the following:

- a) Child pornography - offences relating to child pornography as defined **as: "a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor engaging in sexual activity or depicted in an indecent sexual manner or context."**
- b) Objectionable material - offences relating to the exhibition, sale and other illegal acts relating to **"objectionable films"** and **"objectionable publications"**.
- c) Any other material or activity that involves or is in furtherance of a breach of the criminal law.

Category 2: Extreme

This category involves non-criminal use of material that:

- a) Depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;
- b) Describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or
- c) Promotes, incites or instructs in matters of crime or violence.

Category 3: Critical

This category involves other types of offensive material including any material that:

- a) Has sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults;
- b) Involves racial or religious vilification;
- c) Is unlawfully discriminatory;
- d) Is defamatory;
- e) Involves sexual harassment; or
- f) Brings or has the potential to bring the employee and/or Shire of Northampton into disrepute.

Category 4: Excessive personal use during working hours

This category covers personal use that satisfies the following three criteria:

- a) It occurs during normal working hours (but excluding the employee's lunch or other official breaks); and
- b) It adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties; and
- c) The use is frequent and more than insignificant.

17. Authentication

- a) All passwords/passphrases must expire at regular intervals and have some complexity containing a mixture of numbers, symbols, uppercase and lowercase letters as specified by the ICT Department.
- b) Users must change their password/passphrase when requested by the system or when they feel it may have been compromised.
- c) All passwords/passphrases are to be treated as sensitive, confidential information and must not be shared.
- d) Do not use the 'Remember password' feature of any application for any Shire passwords/passphrases under any circumstances.
- e) Passwords are to be a minimum length of 10 characters.
- f) Paraphrases are to be a minimum length of 14 characters.
- g) Where MFA or 2FA is available to be used for an application or online services, it is mandatory for employees to utilise the authentication method.

18. Remote Access

Remote access is provided to network users by default and by using remote access technology, users must understand that their machines are a de facto extension of the Shire's network, and as such are subject to the same rules and regulations that apply to the Shire's owned equipment. That is, their machines must be configured to comply with this procedure. The employee, contractor, vendor or agent bears responsibility for the consequences if this access is misused.

The following conditions apply to employees, contractors, vendors and agents using remote access:

- a) All requirements outlined in this procedure apply to the use of remote access.
- b) Family members must not violate any of the Shire's policies, perform illegal activities, or use the access for outside business interests. Responsibility rests with the approved user for any consequences that arise from misuse.
- c) The computer that is connected remotely to the Shire's corporate network is not to be connected to any other network at the same time, with the exception of personal networks that are under the complete control of the

- user.
- d) The use of non-Shire email accounts (i.e. Hotmail, Yahoo, and Gmail) or other external resources is not permitted for the conduct of Shire business, thereby ensuring official business is not confused with personal business.
 - e) Non-standard hardware configurations and security configurations for access to hardware must be approved by ICT Department.
 - f) All hosts connected to the Shire's internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers. Third Party connections must comply with requirements.
 - g) Personal equipment used to connect to the Shire's networks must meet the requirements of the Shire's owned equipment for remote access. ICT Department will provide advice regarding current requirements.
 - h) Organisations or individuals who wish to implement non-standard Remote Access solutions to the Shire's production network must obtain prior approval from ICT Department.

19. Termination of Employment

At the termination of employment of a Shire employee, any Shire owned devices will be cleared by ICT, and communications (e.g. email, mobile phone calls) will be redirected as is deemed appropriate.

Administration

This policy will be administered by the Office of CEO.

Adoption and Date Due for Revision

ADOPTED 20 FEBRUARY 2025
REVIEWED N/A

NEXT DUE FOR REVIEW 20 FEBRUARY 2030

The Administration of this Policy is by the Office of CEO.
--

Corporate Policy
2.11
(ICT) System Acceptable Use

APPENDIX

I, _____(please print) acknowledge that I have received training and understand Corporate Policy **2.11 Information and Communications Technology (ICT) Systems Acceptable Use**.

Signature _____

Date _____