POLICY	ROXBY COUNCIL	Responsible Department	Executive
		Original Adoption Date	26.06.19
		Current Adoption Date	**29.06.2022**
		Date of Next Review	30.06.2025

ICT POLICY	
Latest Review Changes	All references to “IT Officer” changed to “Manager IT & Cyber Security”. All references to “Group Manager Corporate Services” changed to Chief Executive.
Previous Council Reviews	26.06.19, 29.06.22

Applicable Legislation

Related Policies (alphabetical list)

Records Management Policy

Related Procedures

Reference Documents

Contents

1. PURPOSE

The Council makes its ICT equipment available to Council staff to enable efficient sharing and exchange of information in the pursuit of Council's goals and objectives.

Council is responsible for maintaining effective security over all equipment and information within its environment.

Due to the portable nature of some ICT equipment, there is a high requirement to maintain security of these devices and for any information stored or transmitted via them.

The purpose of this policy is to provide directives on the deployment, use and maintenance of ICT equipment within the Municipal Council of Roxby Downs so that:

- The correct processes and procedures are drafted and employed when utilising, provisioning and assigning new ICT equipment; and
- Council Staff are aware of their individual responsibilities in relation to the use and security of ICT equipment for the transmission and storage of information and access to the Municipal Council of Roxby Downs systems and infrastructure; and
- Council Staff are aware of the 'appropriate' and 'inappropriate' use of Council's ICT equipment.

2. SCOPE

This policy applies to all users of Council-owned technology, equipment and services. Users could include Council staff, volunteers, trainees, work experience placements, independent consultants and contractors. All rules that apply to the use and access of ICT equipment throughout this policy apply equally to facilities owned or operated by the Council regardless of their location.

The ICT equipment covered by this policy include the following:

- Computers (including notebooks, laptops, tablets);
- Telephones (including mobile and smart phones);
- All software programs associated with Council's ICT equipment, including email systems, internet access, voicemail systems and file storage systems;
- All removable media including CD/DVD, USB devices or any other type of removable media.

3. DEFINITIONS

ICT	Information and Communications Technology
Mobile Phone	a mobile phone is any device that can make or receive phone calls.
Smart Phone	a smart phone usually includes the functions of a mobile phone and extends this to include electronic diary, email, web browsing and a camera.
Mobile Device	a mobile device includes mobile phones, smart phones, iPad or tablet and other mobile devices that have similar functions and access services via wi-fi or mobile data networks.

4. POLICY STATEMENT

To assist Council to meet its Policy Objectives the following sections address the management and use of ICT equipment.

4.1. Management of Mobile Devices

Management of mobile devices is the responsibility of the Manager IT & Cyber Security and overall control is the responsibility of the Chief Executive. This includes:

- Purchasing and applying for newly approved mobile devices;
- Withdrawing and returning mobile devices;
- Assisting Council owned mobile device users;
- Maintaining the mobile device register;
- Reviewing the operation of mobile devices against the ICT Policy;
- Following up maintenance issues;
- Archiving all documentation.

A register of mobile devices will be maintained by the Manager IT & Cyber Security and held on the IT asset register and will include:

- Name of User
- Date Issued;
- History of maintenance required;
- Date for replacement (if appropriate).
- Make/Type/Number/S/N/Pin and PUK numbers

4.2. Provision of Mobile Devices

A Council owned mobile device will only be issued where the applicant can demonstrate sound justification for Council providing a mobile device. Mobile devices can only be approved by the Chief Executive.

Following approval by the Chief Executive the Manager IT & Cyber Security will arrange the purchase of the mobile device and, if required, apply for a mobile service plan. In some cases, existing devices and services may be allocated to the employee if deemed appropriate.

The new mobile device user will receive a copy of the ICT Policy and sign an agreement to abide by the Policy. A copy of the application, approval and signed agreement will be filed in the employee's personnel file.

4.3. Use of Council Owned Mobile Devices

The following must be observed with respect to the use of Council owned mobile devices:

- All use of mobile devices, personally and professionally, must be appropriate and lawful;
- Only mobile devices owned and operated by the Municipal Council of Roxby Downs may be used to connect to Council infrastructure or services without prior approval from the Manager IT & Cyber Security;
- Any installed management software and profiles must not be removed and must be kept up to date;
- Council owned mobile devices remain the property of the Municipal Council of Roxby Downs and as such can be accessed by the Manager IT & Cyber Security upon request;
- Any information which infringes copyright, or any other form of intellectual property rights (e.g. music libraries, movies etc.) is not to be stored on any device owned by the Municipal Council of Roxby Downs;

- The user of the device must notify IT Support immediately upon loss, theft or suspected loss/theft of the device. If necessary, the contents of the device will be remotely erased, and the services associated with the device will be disabled. In the case of theft, the event will be reported to the Police;
- If the mobile device is damaged the user must notify the IT Support who will evaluate the damage and arrange for suitable repair or replacement;
- Council owned devices are locked to the Council's chosen network provider;
- No international calls without prior approval. Usage charges for mobile devices are subject to periodic review. Excess data usage may be investigated and any additional costs that cannot be justified for business purposes may be passed on to the user of the device;
- When using a Council owned device that provides data enabled services, Council staff are required to monitor and manage data consumption levels using the management software provided;
- Council Staff are responsible for ensuring mobile devices are not accessed by other persons that are not authorised to view information on the device.
- USB memory sticks from an unknown or un-trusted source are not to be connected to the Council equipment;

4.4. Use of Non-Council Owned Mobile Devices

Council staff may be permitted to connect non-Council owned mobile devices to the Municipal Council of Roxby Downs systems for the express purpose of receiving email, contact and calendar updates.

In addition to adherence to all other terms of this Policy, the use of a non-Council owned mobile device connected to the Municipal Council of Roxby Downs network, requires acceptance and implementation of the following conditions and shall be confirmed by signature of agreeance to the conditions of this policy:

- The owner/user of the device recognises that there may be voice and data cost implications from using the mobile device for work purposes and that these part of these costs may be covered under the provision of the Council staff allowances;
- The owner/user of the device will accept the installation of a Council-controlled profile, where it is deemed necessary, on the device. The profile will enforce certain configuration parameters including mandatory passcode;
- The owner/user of the device will notify the Council IT Support immediately upon loss, theft or suspected loss/theft of the device. If necessary, the contents of the device will be remotely erased, and the services associated with the device will be disabled;
- The user of the device agrees to protect Council information residing on the device, including ensuring that non-council agents and council agents that are not authorised and do not have access to council information stored on the device;
- No Council data other than mail (including attachments stored within the mail system), contacts and calendar items may be stored on non-Council owned devices unless expressly authorised in writing by the user's Group Manager;
- Non-Council owned devices will not be supported by Council ICT personnel with the exception of connectivity to Council services;
- The Council will accept no liability for functionally, serviceability or performance associated with the device and any responsibility with regard to warranty will reside solely between the owner/user of the device and the supplier/manufacturer;
- The Council accepts no responsibility or liability for the loss of Council related or personally related data residing on the device;
- The Council reserves the right to erase the contents of the device and/or disable the device from Council services at any time, and at its sole discretion.

- The Chief Executive is the authority for any decision relating to the branding mix of Council's mobile devices (e.g. Apple or Android or both), however any such decision should be subject to consultation with the Manager IT & Cyber Security.

4.5. Personal Use of ICT Equipment

Council's ICT equipment is primarily provided for Council's business use and must be used in accordance with this Policy. For Council staff, reasonable personal use of Council's ICT equipment is permissible. However private use is a privilege which needs to be balanced in terms of operational needs. Personal use must be appropriate, lawful, efficient, proper and ethical, and must be in accordance with any Council policy or direction.

Personal Use should:

- Not interfere with staff duties and responsibilities or detrimentally affect the duties and responsibilities of other staff members;
- Not involve activities that might be questionable, controversial or offensive, including gambling, transmitting inappropriate emails or sending of junk programs or mail, and;
- Must not disrupt or place Council's ICT equipment in jeopardy.

Council's computers should not be used for the storage of personal photographs, videos or music. Council may remove these personal files at any stage.

Council's ICT equipment is provided for the staff member only and is not available for use by the staff member's family or friends.

Misuse can damage Council's corporate, business and public image and could result in legal proceedings being brought against both the Council and the user. Council staff reasonably suspected of abusing personal use requirements will be asked to explain such use.

4.6. Inappropriate / Unlawful Use

Under no circumstances shall the Council's ICT equipment be used inappropriately. Inappropriate use includes (but is not limited to):

- Use of Council's ICT equipment to intentionally create, store, transmit, post, communicate or access any fraudulent or offensive information, data or material including pornographic or sexually explicit material, images, text or gather offensive material;
- Gambling activities;
- Representing personal opinions as those of Council, and;
- Use contrary to any legislation or Council policy.

Use of Council's ICT equipment must not violate Federal or State Legislation or Common Law. It is unlawful to transmit, communicate or access any material which discriminates against, harasses or vilifies colleagues or members of the public, on the grounds of:

- Gender;
- Pregnancy;
- Age;
- Race (nationality, descent or ethnic background);
- Religious background;
- Marital status;
- Physical impairment, and;
- Sexual preference or transgender

Please refer to Council's "Discrimination and Harassment Policy and Procedure" for more information.

4.7. Use of Email

In addition to inappropriate usage restrictions for ICT equipment mentioned above, email is not to be used for:

- Non business purposes (e.g. Junk mail);
- Sending or distributing “chain letters”, “hoax” mail or for other mischievous purposes (spam). Only business related subscriptions are permitted;
- Soliciting outside business ventures or for personal gain;
- Distributing software, which is inconsistent with any vendor’s license agreement, and;
- Unauthorised accessing of data or attempt to breach any security measures on the system, attempting to intercept any data transmission without authorisation.

Care should be taken in responding to internal emails addressed to “Everyone” as any responses sent by pressing the “Reply to all” button will be addressed to ALL staff. As such Council staff are advised to take care in writing emails.

Any opinions expressed in email messages, where they are not business related, should be specifically noted as personal opinion and not that of the Council.

4.8. Use of Internet / Websites

It is inappropriate to:

- Intentionally download unauthorised software;
- Download files containing picture images, graphics or videos for personal use;
- Download computer games, music files or accessing TV stations, and;
- Visit inappropriate web sites including online gambling, sexually explicit or pornographic web sites (as previously stated).

4.9. Physical Security of ICT Equipment

The following must be observed when handling ICT equipment:

- ICT equipment must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible, they should be kept on the person or securely locked away, or special cable locking devices should be used to secure the equipment to a non-removable fixture;
- Cable locking devices should also be considered for use with laptop computers or tablets in public places, (e.g. in a seminar or conference, even when the laptop is attended);
- ICT equipment should be carried as hand luggage when travelling by aircraft;
- ICT equipment that contain or have access to Council information must be password protected.

4.10. Protection of Information on ICT Equipment

The following must be observed in order to securely protect information on ICT Equipment:

- Every reasonable effort should be made to ensure that the Municipal Council of Roxby Downs information is not compromised through the use of ICT equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons;
- ICT equipment are not to be used as the sole repository for Council information. All Council information stored on ICT equipment is to be backed up as appropriate.

4.11. Records Management

Any images, texts and voice messages collected on the ICT equipment that relates to Council business and which represents substantive content are considered to be a record and needs to be captured in Council’s electronic records management system.

4.12. Review of Mobile Device Usage

Where the Council pays an ongoing service fee for a mobile device (eg. Voice or 3G/4G data) an annual review of mobile device usage will be conducted by the Manager IT & Cyber Security who prepares a summary report to the Chief Executive to ensure that there is an ongoing business need for the use of each mobile device and that the conditions of the policy are being complied with.

4.13. Withdrawal of ICT Equipment

A Council-owned ICT equipment may be withdrawn for any of the following reasons:

- Misuse of the ICT equipment by the User, which may result in the Council instituting disciplinary procedures against the user;
- Failing to comply with the ICT Policy;
- Non-compliance with conditions specified by the mobile device service provider;
- ICT equipment is no longer required for a certain position or is not being used regularly;
- The ICT equipment user leaves the service of Council.

When disposing of Council's ICT equipment contents of the equipment is securely erased prior to the equipment being disposed of, as of the "Disposal of Land and Assets Policy". The Council does not accept any responsibility for the removal of any employee's personal files that should not be on the ICT equipment.

The user must return the ICT equipment to the Manager IT & Cyber Security with any battery chargers and other accessories, including sim card (when applicable).

4.14. Exemptions

This policy is mandatory unless an exemption is granted by the Chief Executive. Any requests for exemptions from any of these directives should be referred by the Manager IT & Cyber Security.

4.15. Breach of the Conditions of the Policy

In circumstances where a breach of this policy occurs, Council reserves the right to restrict the use or access to the technology or network, equipment or services and to maintain that restriction at its discretion.

4.16. Indemnity

The Council bears no responsibility whatsoever for any legal action threatened or commenced due to conduct and activities of Council Staff in accessing or using these resources or facilities. All Council Staff indemnify the Council against any and all damages, costs and expenses suffered by the Council arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement.

Legal prosecution following a breach of these conditions may result independently from any action by Council.

5. REVIEW & EVAULUATION

This Policy will be reviewed and evaluated no less than once every three (3) years.

6. AVAILABILITY OF THE POLICY

This Policy will be available for inspection at the Council Office at 6 Richardson Place during ordinary business hours and a copy will be available from Council's website https://www.roxbydowns.sa.gov.au.