Council IT and Communications Security Policy

Council Policy

Renmark Paringa Council

Responsible Officer	Director Corporate and Community Services
Relevant Legislation	
Adopted	24 Nov 2015
Reviewed	March 2023
Next Review	March 2025

Objective

Renmark Paringa Council maintains and provides access to Information Technology (IT) and communications equipment and systems in order to meet council's business objectives.

The purpose of this policy is:

- To ensure that any IT asset that stores or accesses Council information is secure
- To minimise the likelihood and impact of incidents on the Council's image, reputation, and business operations.
- To ensure compliance with regulatory requirements.
- To protect information so as to minimise the risk of financial and other loss to the Council
- To establish accountability for employee's actions in regards to protecting, disclosing, accessing, destroying and modifying Council information.
- To support the strategic endeavours of Council by being safe, secure and reliable.

Scope

This policy applies to all Council staff, elected members, volunteers, trainees, work experience placements, consultants, contractors and any other party given access to Council information technology assets or confidential information.

The IT and communications equipment (also referred to as IT equipment within this policy), by definition will include the following:

- Computers (including desktop PCs, thin clients, notebooks, etc.)
- Telephones, and facsimiles,
- Mobile devices (including mobile telephones and tablets),
- Digital cameras and portable USB storage devices, and
- All computer systems and software associated with Council's IT equipment, including email systems, internet access, voicemail systems, cloud systems and file storage systems (onsite and offsite).

All rules that apply to the use and access of IT equipment throughout this policy apply equally to facilities owned or operated by the Council, wherever they are located.

The permitted use of Council's IT equipment must be consistent with other relevant laws, policies and practices regulating:

- Copyright breaches and patents materials legislation,
- Anti-discrimination legislation,
- Council's "Code of Conduct"
- Council's "Social Media Policy"
- Council's "Asset Disposal Policy"
- Practices regulating discriminatory speech and the distribution of illicit and offensive materials, particularly those that are sexual or pornographic in nature

Policy

The Council makes IT equipment available to all Council staff and Elected Members, where appropriate, to enable efficient sharing and exchange of information.

All Council staff and Elected Members have a responsibility to protect Council and to minimise the risk that might result from inappropriate use of council information.

All IT equipment must be secured in accordance with the relevant information security standards and procedures.

Council has implemented a web accessible set of ICT Standards which outline in detail the ICT security policies and relevant forms and procedures to follow.

The ICT Standards are available at https://ictstandards.riverlandcouncils.sa.gov.au:4012Council IT equipment is to be made available to authorised people only, according to least privilege, and must only be used in accordance with the relevant security standards and procedures. Access must be approved by managers.

All Council information rated confidential or internal use only must be protected against intentional or unintentional access or disclosure.

All Council information and systems must be protected and maintained to ensure that integrity is assured.

All Council information and systems must be protected and maintained to ensure that availability is assured.

All access to Council information and systems must be auditable to ensure accountability and non repudiation of actions.

Personal Use

Council's IT equipment is primarily provided for Council's business use and must be used in accordance with this Policy. For Council staff and Elected Members, reasonable personal use of Council's IT equipment is permissible however personal 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 be very infrequent and brief,
- Should not interfere with staff duties and responsibilities or detrimentally affect the duties and responsibilities of other staff members.
- Should not involve activities that might be considered questionable, controversial or offensive including gambling, transmitting inappropriate emails or sending of junk programs or mail, and
- Must not disrupt or place Councils IT 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 IT equipment is provided for the staff member or Elected member only, and is not available for the use by their 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.

Inappropriate/Unlawful Use

The use of Council's IT equipment to make or send fraudulent, unlawful or abusive information, calls or messages is prohibited. Any Council staff who receives any threatening, intimidating or harassing telephone calls or electronic messages should report the incident immediately to the Chief Executive Officer.

Any staff member identified as the initiator of fraudulent, unlawful or abusive calls or messages may be subject to disciplinary action, including under the Council's Code of Conduct for Employees, and possible criminal prosecution, and/or immediate dismissal.