Port Pirie Regional Council

ELECTED MEMBERS COMPUTER, INTERNET & INFORMATION TECHNOLOGY POLICY	
Type	Governance
Category	Corporate & Community
Responsible Officer	Information & Communication Technology Manager
First Issued / Adopted	24 February 2021
Review Period	4 years
Last Reviewed	27 April 2022, 10 February 2021
Minutes Reference	OM 135/22, OM 48/21
Next Review Date	31 July 2026
Applicable Legislation	Local Government Act 1999 Work Health and Safety Act 2012
Related Documents	Elected Member Code of Conduct Elected Members Communication and Records Management Policy
Public Consultation Required	No
File Reference	9.63.1.4

1. PURPOSE

Corporate Information and Communication Technology (ICT) systems are provided as tools to enable Port Pirie Regional Council's business. Council services and supporting processes rely on these systems so it is critical that they are able to operate effectively at all times.

To ensure the Council's IT systems are operated in an effective, safe, ethical and lawful manner it is the responsibility of every computer user to know these requirements and to comply with them.

The purpose of this Policy is to ensure that computers supplied for Council business are managed, maintained and operated in accordance with Council requirements.

2. SCOPE

This policy applies to Port Pirie Regional Council (the Council) Elected Members as users of Information and Communication Technology (ICT) systems and networks owned or managed by Council.

3. DEFINITIONS

Nil

4. POLICY STATEMENT

The Council will provide computers for Elected Members for the purposes of performing their duties. The technology provided will be at the discretion of the Manager ICT and may include a laptop or tablet device and a printer.

Maintenance, troubleshooting problems and upgrades to equipment supplied by the Council will only be carried out by the Council ICT employees. All devices will be centrally managed.

A communication allowance will be provided to Elected Members for the purpose of internet access to enable Elected Members to work at home.

The computers will have the following software installed:

- Windows operating system;
- Microsoft Office;
- An internet browser;
- Printing software.

Elected Members must not install any other software on computing devices.

All equipment is to be returned to the Council when an Elected Member stops providing services to the Council or if required for replacement or upgrading.

Elected Members must not use their personal email address, Facebook page, twitter account or any other form of social media for Council business.

Any social media account set up for the purposes of carrying out the Council's business requires the approval of the Chief Executive Officer and must only represent the Council's position.

A Council email account is supplied by Council for business use only. The address may not be published in any publication or business card that is not related to the Council's business.

Elected Members that also use a computer at home should use different login credentials for Council login and home. Council login passwords need to meet defined complexity requirements and be changed on request from Council ICT employees.

Personally owned communication devices, including mobile phones and tablet devices may not be connected to or synchronised with the Council computer systems or networks unless approved by the Chief Executive Officer and the device owner agrees to the security requirements regarding the management of the device.

Security requirements include:

- Agreement that the device will be managed by Council;
- Agreement for the Council security profile to be applied to the device.

4.1 Computer Systems and Equipment Use

Users of computer systems or networks owned or managed by the Council shall not use these systems to engage in any activity which causes, or could be construed as causing, any form of harassment, discrimination or victimisation of another user including:

- race
- religious belief or activity
- sex
- age
- disability
- industrial association
- lawful sexual activity/sexual orientation
- marital, parental or carer status
- physical features
- political beliefs or activity
- pregnancy and maternity
- personal association with a person who has one of these personal characteristics
- gender
- irrelevant criminal conviction

The computer systems and networks owned or managed by the Council are to be used in an effective, safe, ethical and lawful manner. Misuse of ICT resources will be handled in accordance with existing disciplinary procedures.

Users must not connect personally owned computing devices, computer peripherals, USB devices, digital cameras etc. to computer systems or networks owned or managed by the Council. If Elected Members connect with any personal equipment, this is at their own risk and the Council is not responsible for the device or anything stored on it.

USB sticks or key fobs allocated are only for business use. Extra care is required when storing information on these devices due to their size and portability. Users should be aware of the following:

- Loss of the device and the data is a problem due to the small size
- Increased chance of introducing a virus as they can be used on multiple devices
- Confidential information should not be copied to or stored on a USB storage device
- USBs should not be plugged into any computer that does not have up to date security patches and anti-virus software
- They must be stored and transported in a safe manner to reduce the chances of theft or loss
- USBs containing personally identifiable information (PII) should be protected by means of encryption

Computer equipment supplied by the Council must not be altered or added to in any way including:

- unauthorised upgrades
- addition of components
- removal of components
- altering configuration or security settings
- installation of non-approved applications

All changes to configuration or maintenance of the device must be carried out by ICT employees or their designated agent.

Users must not lend computers, portable devices, tablets, mobile phones, laptops or any other equipment that has been allocated to them by the Council for business activities to anyone external to the Council including friends and family.

Any actions or activities, whether intended or accidental which cause, or could cause the computer systems, information or networks of the Council to be compromised in any way is considered serious misconduct including:

- Security breaches or disruptions of network communications.
- Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
- Port scanning or security scanning. These activities are expressly
- prohibited unless sanctioned by the ICT Manager for the purposes of
- testing network security.
- Executing any form of network monitoring which will intercept data not intended for the employee's device, unless this activity is a part of the employee's normal duties or has been duly authorised.
- Circumventing user authentication or security of any host, network or account or running password cracking programs.
- Interfering with, or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session using any means either locally or externally.
- Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.
- Copying or altering configuration or system files for unauthorised personal use or to provide to other people or users for unauthorised use.
- Creating or using open mail relays maliciously, spoofing mail headers, initiating a mail bomb attack or otherwise interfering with the Council's or another organisation's email service.
- Downloading or introducing tools or utilities that may potentially be used for hacking activities.
- Providing or selling Council information without approval and for personal gain.
- Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using Council resources that would bring the Council into disrepute.

Users must use the standard applications for which the Council is licensed. Do not install any software program, application, script or executable code on equipment in your care. Only software approved by the ICT Manager may be installed on computer equipment owned by the Council and all installations must be carried out by ICT employees.

If printing confidential or potentially sensitive information the following must be observed:

- The person authorised to view the information must be present at the printer during printing to ensure no one else reads the document; or

- The printer is located in a secure area; or
- The document is printed to a storage area on the printer and a code entered or card swiped to initiate the print when the authorised person is present

The same applies to Scanners and Photocopiers.

4.2 Email

The email system is solely for Council business use. Personal use of Council email addresses is not allowed. Misuse will be handled in accordance with existing reference to the Elected Members Code of Conduct.

The email system must not be used for any unlawful activity and must not be used to compromise the security or operation of any computer system or network.

Users must not create, send or forward any email messages that contravene human rights legislation and which may be considered discriminatory, defamatory, intend harassment or hatred on the basis of:

- Race
- Religious Belief or Activity
- Sex
- Age
- Disability
- Industrial Association
- Lawful Sexual Activity/Sexual Orientation
- Marital, Parental or Carer Status
- Physical Features
- Political Beliefs or Activity
- Pregnancy
- Personal Association with a person who has one of these personal characteristics
- Gender
- Irrelevant criminal conviction

Any of the above actions will be handled in accordance with existing disciplinary procedures.

The email system is regarded as an official means of communication and, as such, messages must conform to the same corporate rules for grammar and content as other business communications.

It is not appropriate to use abbreviations (as used in text messages) or profanities, obscenities, derogatory or sexually explicit remarks in business email messages. Such remarks, even when made as a joke, may upset some people. Special caution is warranted because backup and archival copies of email may be more permanent and more readily accessed than traditional paper communications.

Council has a legal requirement to retain corporate email.

Corporate email is defined as:

- E-mail that forms part of an official record. It is email that documents the business activities of the Council, e.g. a direction for an important course of action or business correspondence received from outside the Council

Ephemeral emails can be destroyed as part of normal administrative practice. Ephemeral email is defined as:

- E-mail used to facilitate the Council business but which does not need to be retained for business purposes, e.g., notice of meetings, Elected Member movements, copies of reports or newsletters, advertising material and any other publicly available material.

Files received from an unknown, suspicious or untrustworthy source must be deleted immediately without opening. Under no circumstances should users click on links contained within an email message sent from an unknown source.

4.3 Information Management

All data and information created modified saved, transmitted or archived using the corporate systems of Council remains the property of the Council.

Electronic information must be protected based on its sensitivity, value and criticality regardless of the type of media that holds the information, its location, the systems used to process it or the processes it is subjected to.

The Elected Member must notify the Chief Executive Officer immediately if confidential or sensitive information is lost, disclosed to unauthorised parties, or is suspected of being lost or disclosed.

Users must not delete or dispose of potentially important Council electronic records or information without the approval of the information owner and without following standard document management procedures for disposing of information.

Deleting a Council record without following the proper procedures is considered a serious breach of this Policy.

4.4 Password and Authentication

User IDs and passwords must not be disclosed to anyone or shared with anyone.

Passwords must not be written down and left in a place where unauthorised persons might discover them.

Users that also use a computer at home should use different login credentials for Council and home.

4.5 Backups

Critical information is not to be stored on portable devices, in the unusual instance when this may be necessary, the Elected Member who has the equipment in their care must ensure that the data is backed up. Major changes to critical data should be backed up immediately in addition to any periodic backups. These backups must be stored separately from the device in a safe location and not in the carry bag.

4.6 Reporting Security Incidents

System errors, incomplete updates and processing glitches in software programs or hardware crashes must be promptly reported to the ICT Support Helpdesk.

Users must promptly inform the ICT Support Helpdesk about suspected information security problems including social engineering, virus or malware infection, denial of service, loss or damage to equipment.

Users must report all information security alerts, warnings or suspected vulnerabilities to the ICT Support Helpdesk. Users are prohibited from using Port Pirie Regional Council's systems to forward this information to other users, friends or associates.

Any attempt to interfere with, prevent, obstruct or dissuade an Elected Member that wants to report a suspected information security problem or breach of a Policy is strictly prohibited and will result in disciplinary action.

Any form of retaliation against an Elected Member reporting or investigating information security problems will also be treated as a serious matter.

4.7 Laptop, Tablet and Portable Device Security

Users allocated a laptop or tablet must agree to take responsibility for the security of the device and the information it contains.

Users must not download or install software, freeware or any executable code on a laptop provided to them by the Council. Laptops may only run approved standard applications that have been legally purchased by Council and installed by ICT employees.

Laptops which are occasionally connected to the Council network must meet the following requirements:

- connection is only permitted via authorised and approved facilities
- the laptop must be running up to date anti-virus software and have its firewall enabled
- the laptop must patched up to the current release of the operating system

Users must take good care of their laptops and tablets as they are fragile devices. Damaged equipment must be returned to the ICT Support Helpdesk for repair or replacement.

Laptop and tablet users must ensure that they comply with all information copyright requirements.

Corporate information must be transferred as soon as practical, to the Council corporate systems so records can be saved in the Central Records Database.

A laptop or tablet displaying sensitive information in public must be positioned so that the screen cannot be viewed by others.

Users must avoid situations where theft of the laptop or tablet is possible and take the following precautions:

- Do not leave the device in view in an unattended motor vehicle
- Portable devices must not be left in a vehicle overnight
- The portable device should not be visible from any ground floor window unless there is no alternative
- Secure the portable device when it is not being used

If the laptop or tablet is lost or stolen, this must be reported to the ICT Support Helpdesk immediately. In the event of loss, damage or misuse of any Council equipment, Elected Members may be required to contribute towards replacement or repair or to repay the insurance excess.

Council maintains the right to conduct inspections of any computer equipment it owns or manages with prior notice to the user or custodian.

5. FURTHER INFORMATION

This policy will be available to be downloaded, free of charge, from Council's internet site: www.pirie.sa.gov.au

Copies will be provided to interested parties upon request, and upon payment of a fee in accordance with Council's Schedule of Fees and Charges.