INFORMATION & COMMUNICATIONS TECHNOLOGY POLICY

QUALITY CONTROL			
EDRMS REFERENCES	11/575 – D23/44236		
RESPONSIBLE POSITION	Manager Information & Communications Technology		
APPROVED BY	Council		
REVIEW DATE	26 March 2029	REVISION NUMBER	1
EFFECTIVE DATE	ACTION	MINUTE NUMBER	
26 March 2025	Adoption	47803	

1. INTRODUCTION

The purpose of this policy is to outline the ethical and acceptable use of Broken Hill City Council's (Council) Information Technology (IT) equipment, networks, services and information.

This policy has been adopted to ensure all users have access to a reliable and robust IT environment that is free from malicious and unauthorised use. It aims to cover the rights and obligations of Council, and the rights and obligations of the person using Council supplied technology equipment and services.

This policy, therefore, applies to anyone working at Council, including Councillors, employees, contractors, sub-contractors, third party vendors, external suppliers and authorised personnel (users). Unauthorised users are prohibited from using any Council Information and Communication (ICT) equipment, except equipment specifically supplied for public use.

Council is committed to the appropriate use of technology equipment, resources and services to support and assist with service delivery and business functions across the organisation. IT equipment and services are allocated to Council users to assist in carrying out these functions in an efficient and effective manner.

The purchase and use of technology must always have a central consideration for how it will improve Council's services for the community as well as internal operational, legislative and productivity benefits.

All users of Council supplied equipment and/or services are bound by all applicable current legislation. Council reserves its right to apply any or all parts of the applicable legislation to ensure Council's technology assets and services are used in a manner that complies with legislative requirements.

All authorised users of Council's equipment are required to sign the 'Technology and Services User Agreement' before the use of Council's equipment. Failure or refusal to sign the 'Technology and Services User Agreement' may result in:

- All access to Council's systems being revoked;
- Cessation of Council equipment use; or
- If access to Council's systems or Council equipment use is vital to fulfill the requirements of the role, disciplinary action or grounds for employment/contract termination.

2. POLICY OBJECTIVE

The objective of this Policy is to provide clear guidelines for the correct use and supply of all technology provided by Council for business use.

This policy is in place to protect users and Council. Inappropriate use exposes Council to risks including malicious software, loss of sensitive information, compromise of network systems and services, and legal issues.

Effective security is a team effort involving the participation and support of every Council employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3. POLICY SCOPE

This policy shall apply specifically to all Broken Hill City Council employees and extend to include contractors / sub-contractors engaged by the Council, consultants engaged by Council, visitors conducting business on Council premises, volunteers conducting activities approved by Council, Council Committees and Elected members.

4. POLICY STATEMENT

4.1 Access Control

Before a user can utilise corporate systems, they must have successfully been authenticated as a valid user. Authentication methods will vary across systems and depend on the sensitivity of the information provided. In all possible cases, users must authenticate using accounts that identify the individual. Users are not permitted to utilise logins belonging to other users.

Users are responsible for the actions performed under their account.

Users are only permitted to access information, applications and systems that they have been allocated access rights. Rights are granted based on business need following the principles of least privilege access and the zero trust model.

Authentication credentials (users IDs, passwords, certificates, MFA credentials, physical tokens and access cards) must not be disclosed or shared with anyone. Staff must not share accounts to Council systems unless approval has specifically been obtained from Manager ICT. All authorised shared accounts are documented by Manager ICT.

Only Council owned, or approved external equipment is to be connected to non-public ICT networks and computer systems. Approval can only be gained through Manager ICT.

Where possible and appropriate, authentication must be strengthened with hardening techniques such as multi-factor authentication (MFA), certificate-based authentication and/or other forms of hardening. The decision to implement this requirement must be

based on the risk of compromise, the security classification of the information contained within the system and the capabilities of the system.

Electronic storage of passwords is only permitted in approved encrypted password storage vault solutions. Passwords must not be saved within web browsers, in text files etc. Vault products can only be approved by Manager ICT.

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

Staff must not re-use passwords across multiple services as this allows a single compromise to impact multiple services.

4.2 Communications and Mobile Devices

4.2.1 Email and Communications Activities

When using Council resources to access and use the internet, users must realise they represent Council. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Any form of harassment via email, telephone, or other electronic means, whether through language, frequency, or size of messages.

4.3 IT Equipment

Council undertakes equitable measures to supply equipment and services that are fit for purpose. Council maintains a list of what it deems as standard equipment for supply.

The equipment provided has been chosen to maximise Council's service delivery potential and to be in accordance with Council's procurement policies. Any deviation from the supply of council standard equipment will require a written business case signed and supported by the relevant Senior/Executive Leadership Team member. The models of equipment issued are at the discretion of ICT to ensure maximising return on investment.

Upon employment/contract termination, all council owned equipment issued to users must be returned to council, including but not limited to:

- Laptops, desktops, monitors, keyboard and mouse.

- Portable equipment (mobile phones, tablets, measuring Equipment, IoT devices, scanners, security tokens, physical security passes)External storage devices (USB/Flash Drives)

- All chargers, cases & cords.

Cessation payment/s will be made once all COUNCIL ICT issued equipment is returned to and signed off by the ICT team.

4.4 Internet Usage and Cloud

4.4.1 General Internet Connectivity

Internet connectivity presents Broken Hill City Council with risks that must be addressed to safeguard its vital information assets. Access to the Internet will be provided to users to support business activities as needed to perform their tasks and professional roles. Access to the Internet will be provided to the public as a public service.

All corporate Internet access is explicitly filtered for inappropriate and malicious material and may be subject to intensive monitoring.

All public internet services are provided with limited monitoring in order to protect the privacy of public users and is only filtered to prevent malicious material.

The content filtering is provided on the basis of regularly updated industry blacklists and is not expected to cover all possible sites.

4.4.2 Internet Services Allowed

Internet access is to be used for business purposes and users must limit the amount of time they use the Internet for non-business use. All users must follow corporate principles regarding resource usage and exercise good judgment in using the Internet to ensure cyber security is maintained. Questions can be addressed to the ICT department. Acceptable use of the Internet for performing job functions might include:

- Council business
- Communication between employees and non-employees for business purposes.
- Review of possible vendor web sites for product information.
- Reference regulatory or technical information.
- Research
- Government services
- Council subscribed cloud services

4.5 General Use and Ownership

Broken Hill City Council proprietary information stored on electronic and computing devices whether owned or leased by Broken Hill City Council, the employee or a third party, remains the sole property of Broken Hill City Council.

- You must ensure through legal or technical means that proprietary information is protected and only shared in consideration of the COUNCIL Information Management – Security Classifications section of this policy.
- You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Broken Hill City Council proprietary information.

- You may access, use or share Broken Hill City Council proprietary information only to the extent it is authorised and necessary to fulfill your assigned job duties.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, employees should consult Council's Information & Communications Technology Department.

- For security and systems maintenance purposes, authorised individuals within Broken Hill City Council may monitor equipment, systems and network traffic at any time.

- Broken Hill City Council reserves the right to audit networks, systems and user activities on a periodic basis to ensure compliance with this policy.

4.5.1 Application Usage

Council has many different software applications in use to meet the specific needs of various business units. These applications often contain overlapping feature sets. It is the responsibility of each department and individual to ensure that procedures and policies are followed that relate to the correct usage of each application for their intended purpose.

The ICT department implements standards and offers guidance on the consistent usage of applications across the entire organisation. For example, the Corporate Records Management system is "Content Manager" and must be used for document storage for all Council records, unless a written exemption has been obtained from Manager ICT.

4.5.2 Personal Usage

Using company computer resources to access the Internet for personal purposes must be limited. Personal use must be reasonable and appropriate, not impact on staff productivity or system performance or bring Council into disrepute.

Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Data limits on many of our internet services are not unlimited, and excessive usage can result in large bills. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Where excessive personal usage is identified, usage charges may be passed onto the user.

All users of the Internet should be aware that the corporate network creates an audit log reflecting request for service, both in-bound and out-bound addresses, and can be reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

4.5.3 Unacceptable Usage

Under no circumstances is an employee of Broken Hill City Council authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Council-owned resources.

The following activities are, in general, prohibited. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

Employees may be exempted from these restrictions during-the-course of their legitimate job responsibilities (e.g., ICT staff may have a need to disable the network access of a host if that host is disrupting production services).

- The conduct of a business enterprise, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law.

- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper security controls.

- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

- Any form of gambling.

- Using computers to perpetrate any form of fraud, and/or software, film or music piracy.

- Unauthorised downloading/purchasing/usage of any software, apps or cloud services for use without authorisation in advance from the ICT Department and the user's manager.

- Accessing data, a server or an account for any purpose other than conducting Broken Hill City Council business, even if you have authorised access, is prohibited.

- Loan of allocated mobile devices to others external to Council including friends and family.

4.5.4 Modification

Altering or disrupting IT systems may expose Council to unauthorised information disclosure and introduce additional risks. Users must not perform unauthorised installs or upgrades, remove or modify hardware components including SIM cards, alter configuration or security settings.

Users are permitted to install software and apps from approved curated software catalogues and allow automatic updates to install if prompted.

4.6 Information Management – Security Classification

Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations. Broken Hill City Council uses the following Security Classification scheme.

Official

All information stored, transmitted and processed by Council information systems are classified as Official.

- Official is the default security classification for all information whether the information has been explicitly classified or not.

- Official information by default must remain confidential to Council and not shared with persons outside Council who do not have a need-to-know.

- Information classified as Official must be approved for release to public.

Sensitive

Information requiring additional protection and security and are classified as Sensitive. Highly sensitive or valuable information, both proprietary and personal; must not be disclosed either within or outside the Council without the explicit permission of a member of the Senior or Executive Management Teams (SLT/ELT).

Information classified as "sensitive" includes:

- Personal information

- Health information

- Legal information

- Law Enforcement information

- NSW Government information

- Passwords and private keys intended to protect Council systems and information.

Public

Information intended and approved for public release must carry a classification of "Public". Formal approval and authorisation is required for classifying information as Public.

4.6.1 Classifying Information

The head of each department is responsible for classifying information stored, processed and handled within their department. This may be performed by the establishment of documented business rules for categories of information.

4.6.2 Obligation for Sharing Official Information

Users are permitted to share information that is not classified as sensitive with persons outside Council only when there is a valid business need to do so. The sharing of information classified as sensitive is not permitted without explicit authorisation from SLT/ELT.

Users are to refer to their direct manager if they are unsure about the classification level of information.

4.7 Procurement

IT hardware and software systems may only be purchased or subscribed to with the approval of the Manager ICT to ensure compatibility with Council IT systems, compliance with security, information and records management considerations.

4.8 Remote Access and Mobility

Users of mobile devices must ensure that the device is protected from unauthorised use through locking the device when not in use.

Users need to ensure that the device is secure from oversight and eavesdropping when confidential or sensitive information is being accessed.

Council maintains the right to conduct inspections of any mobile phone or other mobile device that it owns or manages without prior notice to the user. The device must be returned to the ICT department upon request for maintenance and when the user ceases employment at Council.

Mobile devices and communication systems supplied by the Council are provided to facilitate business activities. Reasonable and appropriate personal use is permitted as follows: -

- Minimal calls and text messages
- The data plan must not be exceeded due to personal use
- Personal use must not cause the Council to incur any additional costs or impact staff productivity

Managers will monitor use and may be provided with reports. Personal use may be required to be reimbursed.

A phone supplied by Council may not be used in connection with any personal commercial business activities. The number may not be published in any publication or business card that is not related to the Council's business

4.9 Bring Your Own Device (BYOD)

Personally owned devices may not be connected to or synchronised with Council's computer systems or networks unless approved by the Manager ICT and the device owner agrees to the security requirements regarding the management of the device.

1. Request authorisation from their direct manager and have it approved.
2. Must install a Mobile Device Management (MDM) agent to house and encrypt Council data.
3. Acknowledge that Council is not liable for any problems caused to their personal device, including data loss, as a result of the Council issued Mobile Device Management (MDM) agent being installed.

Council acknowledges the use of personal devices used for business communication; however, Council holds no responsibility for the associated damages, costs and expenses. This includes but is not limited to faulty software, damage to hardware, repairs, bills, applications, games and data usage.

IT team members will always endeavour to assist Council staff wherever possible; however, no responsibility or commitment will be taken for supporting personal devices. Business applications and systems are not guaranteed to be fully compatible with devices of various makes and models other than Council approved devices. Users may therefore experience a reduction in the accessibility and usability of business applications.

Make	Hardware Release Date	Software Release Date
Apple	Less than 5 years	Less than 1 year
Android (Various Manufactures)	Less than 5 years	Less than 1 year

4.10 Cyber Security

Data security is the responsibility of every Council user. All data created or modified whilst employed by Council remains the intellectual property of Council.

All reasonable care must be taken to ensure that the data manipulated using Council equipment is saved in Council's secure storage environment. This environment includes Content Manager, Microsoft 365 and approved cloud systems.

If data is removed from the Council secure storage environment, then the protection of that data is the sole responsibility of the person removing the data.

Loss or misuse of data could in extreme cases be regarded as industrial sabotage, breach of privacy and/or failure in execution of a user's duty of care, leaving the user liable to criminal proceedings.

The connection of portable storage devices, such as external hard drives, USB storage, Flash drives and other storage media to Council equipment introduces security risks for council and is strongly discouraged.

Information stored at council should only ever be used for council business. Storage of personal information on the Council network is prohibited.

Each council officer must ensure that information transferred to portable devices is secure and protected by passwords and/or encryption.

Information transferred to council computers from portable devices must be virus checked before opening.

4.10.1 User Security Awareness Training

Users must complete "Cyber Security Awareness Training" when requested. Council reserves the right to test and measure user's vulnerability against social engineering attacks which includes but is not limited to phishing and vishing simulation. The Cyber Security programme is annually reviewed to ensure effectiveness.

4.10.2 Objectives of Cyber Awareness Training

- Annual re-education and signoff for all employees. > 90% staff attend in a 12-month period.
- Random testing of staff knowledge. Pass rate > 80%. Conducted quarterly.
- Regular dissemination of cyber security information on current risks and strategies to implement for better protection.
- Seeking feedback from staff as to their comfort with Cyber Security practices.

4.10.2 Reporting Incidents

Users must immediately report the following events to ICT:

A. Any form of equipment or data loss such as loss, misplacement or theft of:

   a. Computer equipment (Including Laptops and Desktops)

   b. Portable Storage Devices (Including USB and Flash drives)

   c. Mobile Devices (Including Mobile Phones and Tablets)

   d. Any other device issues by Council to the user.

   e. Loss of security access cards.

B. Loss of information that they previously had access to.

C. Lost access to information that they previously had access to.

D. Access to information that they should not have access to.

E. When they are tricked in clicking on a malicious URL.

F. When they are tricked in opened a malicious attachment.

G. When they are tricked in supplying their corporate credentials.

H. When they notice any change in system security controls such as Anti-Virus software.

4.10.3 Security and Proprietary Information

- Postings by employees from a Broken Hill City Council email address to internet and social media sites is prohibited unless posting is authorised and required in the course of business duties.

- Users must comply with Broken Hill City Council's Password Requirements, including multi-factor authentication adoption in all cases where this is possible, and storage of additional passwords in approved vault products.

- Users are not permitted to connect personal electronic equipment, such as laptops, mobile phones and other BYOD equipment, to Broken Hill City Council's corporate network, without first obtaining authorization from both their direct manager and ICT.

- Once authorized, user must install a Mobile Device Management (MDM) agent, supplied by Broken Hill City Council, to protect and encrypt Council data on their personal electronic equipment.

- User must not provide access to a Broken Hill City Council issued electronic equipment to another individual, either deliberately or through failure to secure its access.

- You must lock the screen or log off when the device is unattended.

- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malicious attachments or hyperlinks to websites that compromise Broken Hill City Council systems.

- The use Broken Hill City Council corporate credentials is prohibited on applications, systems and services, not provided by or subscribed to by Broken Hill City Council.

4.11

Identified breaches of this policy will be handled by the People and Culture department in accordance with COUNCIL's disciplinary policy.

4.11.1 Computer Surveillance

Authorisation to commence surveillance can only be approved by the General Manager. Surveillance can include, but is not limited to, telephone usage reports, security access reports, video surveillance footage, email source and recipients as well as internet usage, internet site visits and network traffic contents. All Council supplied computers produce log files called "Event Logs" which show high level activity and errors. The IT team monitor and use these log files to help diagnose problems, detect security threats, manage individual systems and to help produce statistics on computer usage. These log files do not show personal content and as such are not considered surveillance. The use of these log files does not contravene privacy or surveillance legislation.

4.12 Communication

This Policy will be communicated to staff in accordance with Council's Policy, Procedure and Process Framework. Following approval by the General Manager, the Policy will be made available on Council's intranet.

4.13 Associated Documents

The following documentation is to be read in conjunction with this policy.

D23/44400 – Cyber Security Policy

D23/44649 – Cyber Security Plan

D21/10467 – Cyber Security Framework

5. REVIEW

Review of this policy will incorporate relevant legislation, documentation released from relevant state agencies and best practice guidelines.

The standard review period will be every two years from the effective date. The responsible Council officer will be notified of the review requirements three (3) months prior to the expiry of this policy.

The Manager ICT is responsible for the review of this policy.

6. LEGISLATIVE AND LEGAL FRAMEWORK

This policy is to be read in conjunction with the following:

- ISO27001

- Council employees shall refrain from personal activities that would conflict with proper execution and management of Council's Information & Communications Technology Policy. Council's Code of Conduct provides guidance for recognising and disclosing any conflicts of interest.

7. DEFINITIONS

COUNCIL	Broken Hill City Council
ICT	Information and Communications Technology
Manager ICT	The manager of the Information and Communications Technology department.
MFA	Multi-factor Authentication – a method of strengthening a login process with the requirement to hold two or more credentials to gain access. I.e. a password and a code.
Public Computer System/Network	A system provided explicitly for public use.
Public User	A member of the public, without credentials to access any COUNCIL systems.
Shared Account	An account used by multiple people that doesn't identify a particular user.

Technology and Services User Agreement

I have read, understood and agree to abide by the Broken Hill City Council Information & Communications Technology Policy

Signature:_____ Date:_____

Name of Employee:_____

Department:_____

Please return this signed page to the Information & Communications Technology department, and retain a copy of the policy for your reference.