POLICY

TITLE:	ICT Acceptable Use Policy		
DIRECTORATE:	Corporate Services		
ADOPTED BY:	Chief Executive Officer (CEO)		
DATE OF ADOPTION:	29 Nov 2024	**DATE OF REVIEW:**	29 Nov 2026
POLICY NUMBER:	209		
LEGISLATIVE REF:	*Local Government (General Regulations) 2021; Division 3* *Information Act 2002 (NT)* *Criminal Code 1983 (NT)* *Spam Act 2003 (Cth)*		

1. INTRODUCTION

1.1. Purpose

This Policy outlines Barkly Regional Council's (BRC) expectations and requirements regarding the acceptable security and use of information, data and Information and Communications Technology (ICT) by all system users.

1.2. Scope

This Policy applies to any person who is provided with access to Council systems, referred to throughout this Policy as 'system users'. This includes access to systems at corporate offices, private home or any other location (including working remotely).

This Policy applies to all ICT resources and ICT activities (as defined below).

1.3. Definitions

ICT Resources refer to BRC's computer equipment and software, including any electronic equipment or computer software accessed by system users, inside and outside of working hours, in the workplace or at any other place while performing work for Council. It includes but is not limited to:

- Desktop computers, laptop computers and handheld computing devices
- Printers, scanners, digital cameras or any other digital imaging equipment
- All software and programs provided to facilitate work needs
- Network operating systems including all forms of Email and Internet access
- Any other means of accessing Council's email, internet and computer facilities

ICT activities include, and are not limited to:

- Copying, saving or distributing emails and files
- Access (or attempted access to) and use of data and information
- Downloading, uploading or accessing files from the internet or other electronic sources
- Access (or attempted access to) electronic bulletins, notice boards, blogs and group forums
- Emailing activities and instant messaging via various platforms
- File sharing / File storage / File transfer
- Printing material, Publishing and browsing on the internet
- Streaming media and video conferencing
- Subscriptions to list servers, mailing lists or other like services

A **cyber security event** (or cyber breach) is an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to ICT security.

A **data breach** can harm an individual whose personal information is affected. A data breach happens when personal information is accessed, disclosed without authorisation, or is lost. For example, when:

- A USB or mobile phone that holds an individual's personal information is lost or stolen
- A database or ICT systems containing personal information is hacked
- Someone's personal information is sent to the wrong person

1.4. Responsibilities

All persons within scope of this Policy are required to adhere to this Policy and its associated procedures.

Human Resources is responsible for informing the ICT Department of the requirement to add or remove employees from ICT systems via established procedures.

Other Managers and Directors are responsible for the access and removal of access of system other users which fall under their responsibility.

The ICT Manager is accountable for the overall management of this Policy.

1.5. Policy Objectives

1) Council and system users have an obligation to ensure that it systems ensure the prudent, lawful, effective and safe use and maintenance of data and information contained within its systems.

2) This Policy aims to ensure that Council's ICT systems are not breached.

2. POLICY STATEMENT

2.1 Policy

3) All persons covered by the scope of this Policy are responsible for adhering to the requirements of this Policy and its associated procedures.

4) Council ICT resources must not be used for illegal, inappropriate or improper activities. This includes and is not limited to the access (or attempted access), use, upload, download, sharing or other transmission of pornography, fraudulent activities, gambling, breach of copyright, discrimination, harassment, sexual harassment, bullying, privacy violations and illegal activity including peer-to-peer file sharing.

5) Subject to limited personal use, access to social networks, online professional development, courses or information, discussion groups must be relevant and used only for Council purposes or approved professional development activities.

6) Users must conduct themselves professionally and appropriately when using ICT resources, in accordance with relevant Codes of Conduct and Council policies and procedures.

7) ICT requires notification of the requirement to provide access to ICT resources or installation of equipment as soon as possible, but in any event no later than one week prior to when such access or installation is required.

8) The IT Department will conduct regular data backups to ensure data availability and integrity, with periodic testing to confirm readiness for data loss scenarios. In the event of data loss, a recovery protocol will be followed to restore critical data promptly and minimize disruptions.

9) Multi-factor authentication (MFA) will be required for users accessing Council ICT resources to enhance security. This added layer ensures only authorized individuals can access sensitive information.

3. AUTHORISATION OF USE

System users are authorised to use Council's computer network subject to compliance with the following protocols:

- Prior notice is provided to the ICT Department that a person has been officially employed or otherwise engaged or appointed by the Council;
- A request or authorisation for access to equipment or software has come from an authorised officer;
- The system user is made aware of which computers, software and such other ICT equipment they are entitled to use;
- The system user is hereby made aware of the requirements of this Policy.

4. ACQUISITION, INSTALLATION, MAINTENANCE AND DISPOSAL OF ICT RESOURCES

1) All Council applications, finance applications and business systems used by BRC must be approved, managed, and monitored by the IT Department to ensure security, compliance, and operational efficiency.
2) All procurement of IT assets, including hardware, software, and related services, must be conducted exclusively by the IT department to ensure compliance with security standards, compatibility, and budgetary controls.
3) Access to BRC systems is restricted to authorized personnel, and regular audits will be conducted to verify adherence to security protocols and data integrity standards.
4) Departments must submit requests to IT, which will evaluate and approve acquisitions based on Council requirements and policies.
5) The ICT Department is responsible for the acquisition, installation, maintenance, servicing, repair and disposal of Council ICT resources.
6) Employees must request the ICT Department to acquire and dispose of ICT IT Assets in accordance with established procedures.
7) Under no circumstances must any individual dispose of any ICT assets without following Asset disposal process.

5. USE OF COUNCIL ICT RESOURCES

1) Council ICT resources are provided to users for business purposes. Other than limited personal use, Council ICT resources must be:
    a. Used for business purposes
    b. Used in compliance with all Council policies and procedures
2) System Users are permitted reasonable access to ICT resources to facilitate business communications, provided that use is not unlawful, offensive or otherwise improper.
3) System user identification and passwords must be kept secure and confidential. System users must not allow or facilitate unauthorized access to ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.
4) Active sessions are to be terminated when access is no longer required, and computers secured by password when not in use.
5) Large data downloads or transmissions should be minimized to ensure the performance of ICT resources. Where any person is unsure, they should refer the matter to their Manager or to ICT Services.
6) All system users are responsible for ensuring that they complete their email signature panel as required by Council.
7) All emails sent externally from the Council's systems must automatically have a disclaimer attached to the email as advised by Council.

6. PERSONAL USE OF ICT RESOURCES

1) Users are permitted the limited use of ICT resources for personal reasons provided the use is not excessive and does not breach this Policy.
2) Electronic communications and files (whether they be attachments to email correspondence or created by the user of the ICT resource) that are created, sent or received using Council ICT systems are the property of Council and may be accessed by an Authorised Person or their delegate in the case of an investigation. This includes investigations following a complaint or investigations into misconduct.
3) Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on users' computers, including emails, files and documents are accessible by responsible officers of Council.
4) Any personal use of ICT resources during an individual's working hours must not adversely affect an individual's performance of their duties and should occur while a person is on a break, or as otherwise approved by their Manager.
5) Council may seek reimbursement or compensation from any user for all or part of any costs where the user has caused Council to incur costs as a result of the system user's activities.
6) System users must not use their BRC credentials to create personal accounts on social media or other websites or forums and should avoid re-using their BRC password for any personal purposes.

7. ILLEGAL ACTIVITIES

Use of Council ICT resources must be appropriate to a workplace environment, including strict observation of the following requirements:

- Prohibited access, copying, printing, uploading, downloading or otherwise sharing illegal, offensive or inappropriate material, or saving this onto Council ICT resources; except where such information directly relates to a workplace investigation being carried out by an authorised officer
- Ensuring that ICT resources are not used in any manner contrary to law or likely to contravene any law, regulation, code or guidelines
- No access to unlawful, inappropriate, unauthorised and non-work related use of ICT resources which may constitute a criminal offence under the Criminal Code 1983 (NT). Examples include but are not limited to computer 'hacking', unauthorised release of data, Council material or leaking of information or documents, and the distribution of malware.
- Council ICT resources must not be used to send material that defames (or has the potential to defame) an individual, organization, association, government agency, company or business including Council, its staff and agents, and Elected Members.
- The copyright material of third parties must not be used without authorization. This includes software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text and downloaded information.
- 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).
- Mass electronic communications should only be sent in accordance with normal Council procedures.

8. DATA AND CYBER BREACH RESPONSE

8.1 Data Breach

Under the Act, the Commissioner may serve a compliance notice on Council if it (or its employees or agents) have contravened an IPP, and the contravention is considered to be serious of flagrant or is of a kind that has been done by the organisation on at least 3 separate occasions within the previous 2 years.

For this reason, it is a requirement for service users to promptly report data breaches (as defined) to the IT Department; who will assess and contain the incident to minimize risk. Actions to be undertaken by the IT Department arising from a data breach include:

- Carry out a risk assessment on reported breaches to determine severity, guiding response actions and resource allocation.
- Take any other relevant actions necessary.

8.2 Cyber Security Breach

A cyber security incident is an unwanted or unexpected cyber security event (as defined), or a series of such events, that either has compromised Council operations or has a significant probability of compromising business operations.

System users must report unusual emails, such as spam or phishing, and avoid clicking on suspicious links.

The IT Department will maintain an *Incident Response Plan (IRP)* for managing cybersecurity incidents, focusing on quick containment, data protection and development of cyber resilience.

9. CONFIDENTIALITY AND PRIVACY

Council and its system users are responsible for handling personal information collected through the ICT resources in accordance with the Information Act 2002 (NT), and confidential information as required under relevant Council requirements.

Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of Council ICT resources, this security is not guaranteed, particularly when communicated to an external party.

System users must consider the confidentiality of the material they intend to send when choosing the appropriate means of communication and must determine whether delivery via ICT systems is appropriate.

10. ACCESS AND MONITORING

Authorized Persons may access or monitor Council ICT resources at any time without notice to the user. This includes, but is not limited to, use of Council email systems, and other electronic documents and records and applies to the use of Council ICT resources for personal use.

Authorized Persons may access or monitor the records of Council ICT resources for operational, maintenance, compliance, auditing, legal, employment, security or investigative purposes.

Electronic communications that have been sent, received or forwarded using Council ICT resources, may be accessed and logs of websites visited using Council ICT resources may be generated, examined and monitored.

11. RECORDS MANAGEMENT

Electronic communications are public records and subject to the provisions of the Information Act . System users (in particular Council staff and Elected Members) must store Council records in the designated records management system or EDRMS Platform that Council uses.

It is prohibited to delete or dispose of Council records. Serious penalties apply. Please refer to the *Records Management Policy* for further information.

12. BREACH OF POLICY

System users who are employees are hereby advised that a breach of this Policy may result in disciplinary action, up to and including termination of employment.

Where a criminal offence has been committed this may also be referred to the Police or other relevant authority.

Other system users in breach of this Policy will be managed accordingly.

13. RELEVANT POLICIES

Policies and procedures to be read in conjunction with this policy are:

1) ICT Procedures and Guidelines
2) Incident Response Plan
3) Risk Management Policy
4) Asset Management Policy
5) Codes of Conduct
6) EEO: Anti-Discrimination, Anti-Harassment and Anti-Bullying Policy
7) Social Media Policy
8) Discipline Policy
9) Records Management Policy
10) Confidentiality & Business Policy (Elected Members)

14. IMPLEMENTATION AND REVIEW

14.1. Implementation

Relevant personnel will be made aware of this Policy. It is not a requirement of the Act for this Policy to be published on the Barkly Regional Council website.

14.2. Review

This policy will be reviewed on or before 29 Nov 2026.

15. VARIATIONS, REVOCATIONS AND/OR CHANGES

Barkly Regional Council reserves the right to revoke and/or amend this policy from time to time as is considered necessary to better manage its business and/or to comply with any legislative requirements. Employees will be given sufficient notice of any such revocations, amendments, or changes.

16. APPROVAL

This policy is approved.

Chris Kelly		29 Nov 2024
Chief Executive Officer	Signature	Dated

END