

POLICY

TITLE:	ICT Acceptable Usage Policy		
DIVISON:	Corporate Services - IT		
ADOPTED BY:	Barkly Regional Council		
DATE OF ADOPTION:	August 2020	DATE OF REVIEW:	August 2023
MOTION NUMBER:	OC 271/20		
POLICY NUMBER:	CP 54		
AUTHORISED:	Chief Executive Officer		

THIS POLICY APPLIES TO:
All employees of the Barkly Regional Council

SUMMARY

This policy outlines the Barkly Regional Council's (Council) position regarding the acceptable use of the Information and Communications Technology (ICT) resources by its councillors, employees and sub-contractors and other ICT users.

PURPOSE

Council is responsible for ensuring the use of Council ICT resources is legal, ethical and consistent with the aims, values and objectives of Council and its responsibilities to councillors, employees, sub-contractors and other ICT users.

All users of Council ICT resources are expected to exercise responsibility, use the resources ethically, respect the rights and privacy of others and operate within the laws of the Territory and Commonwealth and the rules and policies of Barkly Regional Council.

Council ICT resources should not be used for inappropriate or improper activities. This includes: pornography, fraud, defamation, gambling, breach of copyright, unlawful discrimination or vilification, harassment, including sexual harassment, stalking, bullying, privacy violations and illegal activity, including illegal peer-to-peer file sharing. The audience of an electronic message may be unexpected and widespread and users should be mindful of this when using Council ICT resources.

SCOPE

This policy applies to all users of Council ICT resources, as defined below, located at corporate offices and in private homes or at any other location (including working remotely). This policy applies to all use of Council ICT resources, including, but not limited to:

- Copying, saving or distributing files
- Data
- Downloading or accessing files from the internet or other electronic sources
- Electronic bulletins/notice boards
- Electronic discussion/news groups
- Email
- File sharing
- File storage
- File transfer
- Information
- Instant messaging
- Online discussion groups and 'chat' facilities
- Printing material
- Publishing and browsing on the internet
- Social networking
- Streaming media
- Subscriptions to list servers, mailing lists or other like services
- Video conferencing
- Viewing material electronically
- Weblogs ('blogs')

NON-COMPLIANCE

Non-compliance with this policy will be regarded as a serious matter and appropriate action will be taken, which may include termination of employment.

Depending on the nature of the inappropriate use of Council ICT resources, non-compliance with this policy may constitute:

- A breach of employment obligations
- A breach of the employee code of conduct
- A criminal offence
- A threat to the security of Council ICT resources and information
- An infringement of the privacy of staff and other persons
- Exposure to legal liability
- Serious misconduct
- Sexual harassment
- Unlawful discrimination.

Where there is a reasonable belief that illegal activity may have occurred, this will be reported to the CEO and may be reported to the Northern Territory Police and/or Australian Federal Police.

USE OF COUNCIL ICT RESOURCES

Business Purposes

Council ICT resources are provided to users for business purposes. Other than limited personal use, Council ICT resources must be:

- Used for business purposes, or where authorised or required by law.
- Used like other business resources and users must comply with any Council codes of conducts or legislative requirements that apply to the user.

Users are allowed reasonable access to electronic communications using Council ICT resources to facilitate communication between employees and their representatives, provided that use is not unlawful, offensive or otherwise improper. This may include a union on matters pertaining to the employer/employee relationship.

Large data downloads or transmissions should be minimised to ensure the performance of Council ICT resources for other users is not adversely affected.

Personal Use

Users may use Council ICT resources for personal reasons provided the use is not excessive and does not breach this policy. Excessive personal use during working hours covers personal use which satisfies the following criteria:

- Occurs during normal working hours (but excluding an employee's lunch or other official breaks);
- Use adversely affects, or could reasonably be expected to adversely affect, the performance of the employee's duties; and
- The use is not insignificant.

Council may seek reimbursement or compensation from a user for all or part of any costs where the user has caused Council to incur costs due to excessive downloading of non-work related material in breach of this policy.

Subject to limited personal use, social networking, on-line conferences, discussion groups or other similar services or tools using Council ICT resources must be relevant and used only for Council purposes or professional development activities. Users must conduct themselves professionally and appropriately when using such tools.

When subscribing to mailing lists and other like services using Council ICT resources, the user must use a different password and logon credentials to their Council logon credentials and passwords.

Users should be aware that the provisions applying to access and monitoring of Council ICT resources also apply to personal use.

Defamation

Council ICT resources must not be used to send material that defames an individual, organisation, association, company or business; this includes the council, both staff and elected members.

Copyright Infringement

The copyright material of third parties must not be used without authorisation. This includes software, database files, documentation, cartoons, articles, graphic files, music files, video files, books, text and downloaded information.

Illegal use and material

Council ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender may be referred to the police or other relevant authority and their employment may be terminated.

Certain inappropriate, unauthorised and non-work-related use of Council ICT resources may constitute a criminal offence under the Criminal Code Act 1983 (NT) Examples include computer 'hacking', unauthorised release of data, Council material or leaking of information or documents and the distribution of malware.

Offensive or inappropriate material

Use of Council ICT resources must be appropriate to a workplace environment and aligned to Council's Code of Conduct. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.

Offensive or inappropriate material must not be forwarded internally or externally, or saved onto Council ICT resources, except where the material is required for the purposes of investigating a breach of Council policies.

Attribution

Users are accountable for all use of Council ICT resources that have been made available to them for work purposes and for all use of Council ICT resources performed with their user identification. Users must maintain full supervision and physical control of Council ICT resources at all times, including mobile phones, tablets and notebook computers.

User identification and passwords must be kept secure and confidential. Users must not allow or facilitate unauthorised access to Council ICT resources through the disclosure or sharing of passwords or other information designed for security purposes.

Active sessions are to be terminated when access is no longer required and computers secured by password when not in use.

Mass Distribution and Spam

The use of Council ICT resources for sending 'junk mail', for-profit messages, or chain letters is strictly prohibited.

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.

CONFIDENTIALITY AND PRIVACY

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. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

Council will handle any personal information collected through the use of Council ICT resources in accordance with the Information Act 2002 (NT) and Privacy Act 1988 (Cth).

COUNCIL PROPERTY

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.

Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on users' computers, including emails, may be accessible under the Information Act 2002 (NT).

Email messages may be retrieved from back-up systems.

EMAIL DISCLAIMER

All emails sent externally from the Council emails will automatically have a disclaimer attached to them.

The use of the email disclaimer may not necessarily prevent Council or the sender of the email from being held liable for its contents.

ACCESS AND MONITORING

Authorised 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.

Authorised Persons may access or monitor the records of Council ICT resources for operational, maintenance, compliance, auditing, legal, 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.

RECORDS MANAGEMENT

Electronic communications are public records and subject to the provisions of the Information Act 2002 (NT).

RELEVANT POLICIES

Policies to be read in conjunction with the Barkly Regional Council Code of Conduct:

- Barkly Regional Council Social Media Policy
- Barkly Regional Council Code of Conduct
- Barkly Regional Council Employee Grievances and Dispute Resolution Policy
- Barkly Regional Council Anti-Discrimination Policy
- Barkly Regional Council Bullying and Harassment Policy

IMPLEMENTATION AND DELEGATION

This ICT acceptable use policy applies to all users of Council ICT resources. This policy is delegated to the CEO for implementation.

VARIATIONS, REVOCATIONS AND/OR CHANGES TO THE CODE OF CONDUCT

Barkly Regional Council's reserves the right to revoke and/or amend the ICT acceptable use 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.

Acknowledgement

I, _____ (*Print full name*) have read and understood the Barkly Regional Council ICT acceptable use policy and I agree to abide by this policy which is outlined above.

Employee signature: _____ Date signed: _____