3.18 USE OF COUNCIL ICT RESOURCES

Council Resolution:	**19/02/2013/007**
Date to take effect:	20 February 2013
Legislative reference:	*Local Government ACT 2019*
Review Date:	June 2024

1. Purpose

This policy establishes the parameters under which staff members, contractors and volunteers at Coomalie Community Government Council are expected to behave while accessing and using Council ICT resources to ensure that use is legal, ethical and consistent with the aims, values and objectives of Council.

This Policy applies to all users of Coomalie Community Government Council ICT resources regardless of work location and to all ICT resources, devices and services including:

- Software applications and services and the data they contain, including email;
- Desktop computers, peripherals and devices; and
- Telephones, radio systems, IoT networks, faxes, data and internet connections; and
- Mobile devices such as laptops, tablets and smartphones provided by Council;
- Personally, owned devices connected to Council resources; and
- Network, server, storage (including USB) and cloud resources.

2. Principles

This policy seeks to:

- Establish the conditions under which a user can access Council ICT resources.
- Mitigate the risks of providing access to corporate ICT resources to a wide range of users while maintaining a secure communications and computing environment; and
- Ensure the rights and responsibilities of both Council and the staff member are appropriately protected from the misuse of Council ICT resources.

3. Policy Statement

3.1 Authorised Use of Council ICT Resources

A wide variety of systems are employed across Council operations and are fundamental in carrying out the role of local government for our community. At all times are, use of Council ICT resources is subject to the applicable Code of Conduct. There are two authorised uses of Council ICT resources:

3.1.1 Business Purposes

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

- Used for business purposes only, or where authorised or required by law, or with the express permission of an Authorised Person.
- Used like other business communications and comply with any codes of conduct 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.

3.1.2 Personal Use

Limited personal use of Council's ICT resources is allowed provided the use is not excessive and does not breach this policy or adversely affect the performance of the employee's duties, or the ability for Council to operate effectively.

3.2 Unacceptable Use

In order to ensure Council ICT resources are safe, secure, and do not pose a risk to Council or the community, the following activities are not acceptable and may result in disciplinary action up to and including termination and/or prosecution.

3.2.1 Excessive Personal Use

Excessive use of Council ICT resources is defined as “personal use” which:

- Occurs during normal working hours, but outside of employee breaks;
- Adversely affects the performance of the employee’s duties, or adversely affects the ability for others to do so;
- Is significant and consistent.

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.

3.2.2 Unauthorised Access

Obtaining unauthorised access to electronic files of others or to email or other electronic communications of others, is not permitted and may constitute a criminal offence. This includes the sharing of passwords to others both internally and externally to Council.

3.2.3 Copyright Infringement

The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and downloaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or Council liability, despite the belief that the use of such material was permitted.

Council supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.

3.2.4 Defamation

Council ICT resources must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or Council liability.

3.2.5 Illegal Material

Council ICT resources must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and will be viewed as a serious breach of the terms of employment and appropriate action taken.

Illegal or unlawful use includes but is not limited to use of certain types of pornography, defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking, use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under various Crimes Acts or any other relevant legislation.

3.2.6 Offensive or Inappropriate Material

Council ICT resources must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually oriented messages or images and messages that could constitute sexual harassment.

Users of the ICT resources who receive unsolicited offensive or inappropriate material electronically should notify their manager. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of the material should be asked to refrain from sending such material again. Such 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 this policy.

3.2.7 Spam and Mass Distribution

The use of electronic communications for sending unsolicited commercial electronic messages ‘Spam’, ‘Junk Mail’, for-profit messages, or chain letters is strictly prohibited and may constitute a breach of the Spam Act 2003 (Cth).

Mass electronic communications should only be sent in accordance with Council’s normal procedures and practices. Where possible a 3rd party program should be used for mass communication via email to avoid the potential of exposing Council’s email system to blacklisting.

3.2.8 Social Media

Only employees with authorisation may use social media for Council purposes. All other staff should use social media for their personal use sparingly throughout the workday. Unless authorised, commenting on Council related issues through social media at any stage is not acceptable.

3.3 Mitigating Risk

All users of Council ICT resources have a role to play in mitigating and minimising risk to the organisation.

3.3.1 Council Owned Property

Council is the owner of and asserts copyright over:

- All electronic communications created by employees as part of their employment and sent through Council ICT resources.
- All electronic data/information stored on Council ICT resources.

Electronic communications created, sent or received by the users are the property of Council, and may be accessed as records of evidence in the case of an investigation. Electronic communications may also be subject to discovery in litigation and criminal investigations. Email messages and mobile phone text messages may be retrieved from back-up systems.

3.3.2 Passwords and Access

Users are accountable for all use of Council ICT resources that have been made available to them for work purposes. Users must maintain full supervision and physical control of Council ICT equipment, including notebook computers and mobile phones, at all times. User-IDs and passwords must be kept secure and confidential. User-IDs and passwords should not be disclosed to anyone, including managers or above. Active connections to systems and data are to be terminated when access is no longer required, and PCs secured by password when not in use.

3.3.4 Your Personal Information

Council will use personal information about you including your name, position, staff number and business contact details (email, phone, location) to provide ICT

services. When you voluntarily provide other information such as your personal mobile number and/or email address to Council, you agree that this information may also be used to provide ICT services. This may include testing, training and support of ICT resources, which may be carried out on premises or in outsourced arrangements with approved service providers.

Council will not release your personal information unless required to do so under law.

3.3.5 Your Personal Devices

Where personal devices are used to access Council ICT resources, any information, data, communication or transmission using Council ICT resources remains the property of Council. This includes text messages, emails, files and applications licensed and provided by Council for business use. This does not imply control over the device itself, nor does it reduce the responsibility of the individual for use of the device contrary to this Policy.

3.3.6 Viruses

Viruses have the potential to seriously damage Council ICT resources. Downloaded files, emails or attachments that you are not expecting or that look suspicious should not be opened. In the event that a file is received that is suspected to contain to a virus it should be reported immediately to the IT Manager.

Electronic communications are potential delivery systems for various forms of computer viruses. All data, programs and files which are downloaded electronically, attached to messages or imported on any other media (e.g. thumb drives, flashcards, iPods, removable disks, cameras) will be scanned by an anti-virus program before being launched, opened or accessed.

3.3.7 Monitoring

Use of Council's ICT resources constitutes consent to monitoring in accordance with this Policy. From time to time, Authorised Persons may examine or monitor the records of Council ICT resources for operational, maintenance, compliance, auditing, security or investigative purposes. This may occur without your knowledge. The CEO has authority to suspend or terminate all or any part of a person's use of Council ICT resources based on the suspicion or having evidence of potential breaches.

3.4 File and Document Storage

All Council documents received, produced or shared during the course of Council operations are to be stored in the central file location provided by the IT Manager, where they are able to be secured, managed and shared in a systematic manner.

3.4.1 Business Classification

Files and documents are to be stored according to the functional/organisational use or purpose as defined in Coomalie Community Government Council Business Classification Guide. Doing so ensures:

- Appropriate filing of both internally generated and externally received documents and files takes place;
- Council is protected from the loss, both intentional and unintentional, of organisational records;
- Accurate and consistent file keeping standards are maintained;
- Staff are able to find and use information during the course of their work.
- A core set of corporate data is maintained;
- Records management is compliant with the requirements of State Archives.

4.0 Permission Structures

Permissions are maintained by the IT Manager in order to ensure confidential and sensitive information is secured in a manner compliant with legislation and are approved by the Executive Manager Finance and Human Services. These permissions are maintained in a suitable register, and regularly reviewed.

5.0 Responsibilities

CEO, Directors and Managers are responsible for:

- Ensuring all those individuals covered by this Policy have access to this Policy and the associated Guideline
- Providing regular updates, training and compliance reviews

IT Manager is responsible for administering the necessary technical requirements to ensure the requirements of this Policy are met, as well as maintaining the Business Classification Guideline.

All users covered by this policy are responsible for:

- Reading, regularly reviewing, and maintaining compliance with this Policy.

Exceptions to this Policy are approved only in writing by the Chief Executive Officer or their delegate.

1. Related Documents

1. *Staff Benefits Policy.*
2. *Employee Code of Conduct*

DOCUMENT HISTORY **3.18 USE OF COUNCIL ICT RESOURCES**		
Date Adopted:	05/08/2003	19/02/2013/007
Amended:	February 2019	19/02/2019/016
Amended:	July 2020	21/07/2020/019
Amended:		