INFORMATION TECHNOLOGY RESOURCES POLICY

CORPORATE SERVICES
YASC C-POL 32 – V3

2026

YARRABAH ABORIGINAL SHIRE COUNCIL
56 Sawmill Rd Yarrabah, QLD 4871

CONTENTS

1. LEGISLATION AND AUTHORITY 2
2. COUNCIL'S STATEMENT 2
3. PURPOSE 2
4. COMMENCEMENT OF POLICY 2
5. DEFINITIONS 2
6. ROLES AND RESPONSIBILITIES 3
7. COMPUTER SOFTWARE AND HARDWARE 3
8. REPLACEMENT PROCEDURE FOR HARDWARE 5
9. TRAINING 6
10. REVIEW TRIGGER 6
11. PRIVACY PROVISION 6
12. VARIATIONS 6
13. DOCUMENT CONTROL 6

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

1. LEGISLATION AND AUTHORITY

The Local Government Act 2009 (Qld)
Local Government Regulation 2012 (Qld)
Public Records Act 2009 (Qld)
Right to Information Act 2009 (Qld)
Information Privacy Act 2009 (Qld)
Privacy Act 1988 (Cth)

2. COUNCIL'S STATEMENT

Yarrabah Aboriginal Shire Council *('Council')* conducts its business with integrity, honesty and fairness. All employees are expected to work within the rules and actions of Council will comply with all relevant laws, regulations, codes and corporate standards.

Everyone representing Council must reflect the highest standards of behaviour. Our relationships are critical to the ongoing success of our organisation. Our leaders have responsibility for fostering a culture where ethical conduct is recognised, valued and applied at all levels.

This policy is to be read in conjunction with relevant legislation and the Code of Conduct, which outlines our standards of behaviour and workplace culture are in accordance with Council's principles:-

PURPOSE

Yarrabah Aboriginal Shire Council (Council) is a highly computerised organisation with various hardware and software resources being used to undertake core functions of Council.

This document describes the user and the management responsibilities when using these resources, as well as the best practice procedure for the various IT resources.

This document also discusses the replacement and renewal of the IT Assets and their effective disposal.

3. COMMENCEMENT OF POLICY

This Policy replaces all other Information Technology Resources policies of YASC (whether written or not).

4. DEFINITIONS

IT Officer:- The term IT Officer refers to an employee of the organization or contracted third party service provider, tasked with the responsibility of administering all aspects of Council's information technology platforms.

Resources - The term Resources refers to anything owned, controlled or paid for by the Council regardless of its state of repair or future use within the organisation. This includes, but is not limited to:

Physical Resources such as:

- Equipment e.g., Computer equipment, software, power tools, machinery, cameras, motor vehicles, fuel,
- spare parts and accessories, office equipment and stationery, consumable materials used in a process, off-cut materials
- Surplus materials that have been costed but not used on a project
- Waste products able to be recycled

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

- Recyclable materials and items – including metals
- Packaging and storage items
- Materials subject to deterioration, which are regularly replaced to maintain safety or
- quality standards.
- Perishable items that have exceeded their used by date.
- Items in good condition, but deemed unusable due to circumstance
- Damaged, inefficient, or non-working items considered to be uneconomical to repair
- Items of low value that are not controlled by the asset register
- Assets originally of high value that have diminished in value over time

Intellectual Resources such as:

- Council correspondence, reports or records (other than those documents on the public record).

Financial Resources such as:

- Petty cash, purchase orders, purchasing identification cards

People Resources such as:

- An employee's work time or the work time of others

Natural Resources such as:

- Water, trees, shrubs, seedlings and flowers

Mobile Device - A portable computing device such as a smart phone or a tablet computer

6. ROLES AND RESPONSIBILITIES

This policy applies to:

- Any person, whether a permanent, temporary, contracted, casual employee, Councillor or trainee of Council who has access to Council's IT resources
- All guests/visitors of the Council
- Any other authorised users or organisations accessing Council's resources

7. COMPUTER SOFTWARE AND HARDWARE

The Council provides computer hardware and the software to enable the staff and the Councillors to perform their various functions within the Council.

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

7.1 **Software**

All software installed in Council computers (desktops or notebooks) must have valid licences. Council is liable for any illegal software installed on computers. The IT Officer must be notified, and licences verified prior to the installation of any software on Council computers.

Any new software is to be validated by the IT Officer without exception. All the software will be validated by Council's Managed Services Support to check whether they are compatible with cloud environment and then will decide whether they have to be installed locally or on to the cloud.

Personal software must not be installed on Council computers. The IT Officer or Support Services undertakes audits for inclusion in the IT Software Register. Any illegal software found will be uninstalled and notified to the Director Corporate Services.

7.2 **Hardware**

Hardware includes the computers (desktop or notebook) equipment and attached peripherals including keyboard, mouse, printer, audio devices, mobile phones, iPads/Tablets, hard drives, UPS.

The Staff and the Councillors are responsible for the good care of their equipment. Faults or problems must be reported to the IT Officer as soon as practical.

All purchases or acquisitions of hardware must be validated by the IT Officer without exception. The IT Officer should undertake annual audits and checks for inclusion/exclusion in the IT asset register.

7.2.1 **Mobile Devices**

7.2.1.1 Issuing and Return of Mobile Device

The mobile device will be issued to staff based on their position description or on an email from the CEO. The person to whom the mobile device has been issued, will be responsible for any damage or theft. Each person who is issued with a mobile device should sign a mobile devices agreement form Appendix 3 and should abide to the terms and conditions as set out in the form. The mobile device and all the accessories (cover, sim card, transfer cable and charger) are assets owned by the Council and must be returned to the issuing Officer if personnel resign.

If the person decides to keep the mobile device, the amount equivalent to the market price must be paid to the council.

Staff are not permitted to keep the Council service number (mobile no.).

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

7.2.1.2 Theft and Accidental Damage

In case of theft the Director of Corporate Services must be notified immediately in order that the required actions will be taken. Any damages to the mobile device will be considered for repair if possible.

In both the cases, the costs will be invoiced to the users.

8. REPLACEMENT PROCEDURE FOR HARDWARE

8.1 Scope

This section implies how the IT hardware including the computers/laptops, printers, UPS and mobile devices are replaced.

8.2 Renewal Plan

The assets requiring renewal are identified from the IT Asset Register (annually updated) based on the life and warranty of the asset or upon a reasonable request from the users Manager. The assets that require general replacement are to be budgeted for approval. The useful life and warranty of assets can be found in the Appendix 1.

8.2.1 Outdated Hardware

a) The hardware to be replaced should be identified from the Asset Register. The majority of hardware are purchased with a 3-year warranty.
b) After the three-year warranty period, if the hardware is found to have no issues, it is not then considered for replacement until it reaches its useful life period or in case of significant issues hardware replacements are done. Please refer to Appendix 1
c) In case of the mobile devices, they will not be replaced within three years unless a malfunction has occurred.
d) Hardware being replaced is to be returned for the Director of Corporate Services to dispose of as per the Asset Disposal Policy

8.2.2 Malfunctioning Hardware

a) Any malfunctioning hardware is to be reported to the IT Officer.
b) The IT Officer will arrange inspection and will send the hardware away for repairs, if economically repairable.
c) Where it is not economically practical for repair, it will be considered for replacement.

8.2.3 Hardware Renewal Requests

a) All the Managers and relevant staff are provided with laptops. If any other user having a desktop wants to swap with a laptop, a business case to be put forward through their respective Manager.

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

b) All the Managers and relevant staff may be provided with a mobile phone with a basic configuration.
c) In case of the renewal requests for laptops and computers with higher configuration from the users, a Request for Renewal Form (Appendix 2) should be submitted to the IT department after authorisation from their respective Manager.
d) However, after considering the requests, the IT department has the right to decline if the request is not reasonable.

9. TRAINING

For Software - training will be provided for Council issued software; based on the user's previous knowledge and level of usage of the software.

For Hardware - training will be provided on the usage of the hardware which includes desktop/laptop, printers and mobile devices on request by the users.

10. REVIEW TRIGGER

Policy is to be reviews every 2 years.

11. PRIVACY PROVISION

Council respects and protects people's privacy and collects, stores, uses and discloses personal information responsibly and transparently when delivering Council services and business.

12. VARIATIONS

Council reserves the right to vary, replace or terminate this policy from time to time.

13. DOCUMENT CONTROL

Adoption Date:	13 November 2023	Resolution No. 04:25/10/2023	Version No. 1
Reviewed Date:	26 July 2024	Resolution No. 12:26/07/2024	Version No. 2
Reviewed Date:	19 August 2026	Resolution No. 28:19/08/2026	Version No. 3
Next Review Date:	2027		
Responsible Officer:	Chief Executive Officer		

Richard Wright
Chief Executive Officer

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

APPENDIX 1

CATEGORY	WARRANTY	USEFUL LIFE
Monitors	3 years	4-5 years
Desktops/Laptops	3 years	4-5 years
UPS	2 years	End of life
Printers	3 years	5-6 years
Mobile devices	2-3 years	3 years
Photocopiers	Life of lease	
Auxiliary Equipment		5-7 years

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

APPENDIX 2

Request for Renewal Form

NAME: DATE:

POSITION:

SUPERVISOR:

DEPARTMENT:

REASON FOR RENEWAL:

EMPLOYEES SIGNATURE: SUPERVISOR/MANAGER SIGNATURE:

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.

APPENDIX 3

MOBILE DEVICES AGREEMENT

1. The mobile device provided is your own responsibility.
2. The device should be password protected and the password must not be shared.
3. Sensitive data should not be copied or stored in unapproved applications on the device and is restricted to share with unauthorised persons.
4. Any loss or damage to the device to be reported immediately and the damage or loss will be costed to your account based on the market value.
5. No calls to be made from the I Pads or Tablets. Any excess charges to the mobile data or personal calls will be charged to respective accounts.
6. Download of malware and content from the illegal websites on the device is prohibited.
7. At any point of time the mobile device should not contain any offensive images or texts, material of sexual nature, indecent or pornographic material and gambling websites.

I abide to the above-mentioned conditions.

Name: Date:

Signature:

This is a controlled document. It becomes uncontrolled when printed or copied, unless manually signed by the Authorising Officer.