Toukley Neighbourhood Centre
Ph: 02 43961555 / Email: admin@tnc.org.au / Website: www.tnc.org.au
PO Box 55, Toukley NSW 2263 / ABN: 64 997 484 484 / Association No: Y02437-47

TNC is the heartbeat of a connected, supported, empowered, inclusive and thriving community. We partner with the broader community to share what we can and provide a hand up to those in need, so they can Wallamba-bayn (come back) and join us in delivering our vision.

POLICY – ELECTRONIC MEDIA

1. Policy Information

Title:	Electronic Media
Effective Date:	19-Jan-2026
Policy Owner:	Executive Officer
Oversight:	Risk & Compliance Committee
Next Review Date:	Jan-2027

1.1. Definitions

This policy uses the terms defined in the *TNC Master Definitions Table*, available on the Toukley Neighbourhood Centre website (www.tnc.org.au/policies).

Policy-specific definitions are listed below (if required).

Term	Explanation
ACNC	Australian Charities and Not-for-profits Commission
Associated Tools	Refers to technology required to access Electronic Media such as: • Computers • Phones • POS devices Tablets.
BoM	Board of Management
Electronic Media	Includes, but is not limited to: • Email • Instant messaging and chat facilities (e.g. MS Teams) • Internet • Online discussion groups SharePoint.
EO	Executive Officer
IT	Information Technology
MS	Microsoft
NFP	Not for Profit
POS	Point of Sale
TNC	Toukley Neighbourhood Centre

1.2. Context

At Toukley Neighbourhood Centre (TNC), policies are developed in alignment with the *TNC Policy Framework* and support the delivery of safe, effective and accountable community services.

TNC policies are developed to:

- Assist TNC to meet its organisational objects and manage risk effectively
- Support staff and volunteers in performing their duties
- Demonstrate how TNC meets its governance, compliance and quality expectations
- Provide clarity, transparency and consistency across all areas of TNC operations.

TNC is bound by the *Australian Charities and Not-for-profits Commission Act 2012 (Cth)* and regulated by the *ACNC*.

1.3. Related Documents

- Cybersecurity Policy
- Privacy and Data Protection Policy
- Records Management Policy

1.4. Change Control

Effective Date	Author	Approver	Comments
12-Dec-2023	Bronwyn Evans	BoM	Initial document
08-Apr-2024	Bronwyn Evans	BoM	Forbid the use of USB storage devices, action arising from Loyal IT Cyber Security Audit.
09-Dec-2024	Donna Tudman	BoM	Annual review and minor refinements to RACI
19-Jan-2026	Bronwyn Evans	BoM	• Apply new template and complete new sections • Update to Executive Officer (EO), formerly Centre Manager (CM) • Remove measurement criteria • Clarified BYOD expectations for use of personal devices to access TNC electronic media and systems

1.5. Contents

2. Policy Overview

2.1. Purpose

This policy sets out the guidelines for acceptable use of electronic media and associated tools. Staff and volunteers are provided with these resources for the primary purpose of assisting them in carrying out their duties.

2.2. Overview

TNC recognises that staff and volunteers may need access to electronic media and associated tools to successfully fulfill their role. In addition, staff and volunteers should have access to reasonable personal use of these resources whilst working for TNC.

2.3. Scope

This policy applies to all TNC staff, volunteers, contractors, students, and any other individuals engaged in TNC activities.

It applies to all TNC programs, services, premises, digital systems, equipment and activities unless otherwise stated within this policy.

Policy-specific scope requirements or exclusions are detailed below (if applicable).

- This policy governs the acceptable use of electronic media and associated tools, including where personal devices are approved for access. Technical security requirements for devices, systems and accounts are governed by the Cybersecurity Policy.

3. Policy Principles

Policies always contain a set of principles that provide information relating to the rationale for the document. Staff and volunteers must consider and comply with these guiding principles when performing their duties.

Principle 1: All TNC activities must be conducted using TNC accounts

TNC activities must be undertaken by suitably authorised and acknowledged staff and volunteers. The use of personal accounts, even if "TNC" is included in the account name, is unprofessional and carries risk and thus forbidden.

Specifically, this means:

- Everyone who requires access to technology for TNC purposes must be allocated a TNC email account.

  TNC has NFP licensing for Microsoft 365. Permanent staff will be allocated a TNC Business Premium license. The NFP grant allows for ten licenses, and this accommodates staff and some generic email addresses (admin, reception and some programs).

  All casual staff and volunteers with a requirement to access technology resources will be allocated a Business Basic license. The NFP grant allows up to 300 such licenses, which is more than sufficient for our uses.

  When staff and volunteers leave the organisation, their TNC email addresses must be cancelled within five working days.
- Access to online services / systems must be conducted with a TNC email address.

  This gives TNC IT Support control over who has access to these systems as these email addresses can be terminated if required.

  For clarity, access to online services / systems is not to be conducted using personal email addresses, or pseudo-TNC email addresses (e.g. TNC@gmail.com).
- Generic TNC email addresses are used for online services that require an account owner or where multiple people share the account. Generic TNC email addresses are also promoted externally to the organisation to remove the reliance on an individual (who may not be available, may have left the organisation or may have changed role).

  Examples:
  - TNC website should direct email enquiries to the generic TNC email address that is responsible for triaging enquiries.
  - Arlo Security system has an account owner to manage the subscription, cameras and monitoring schedule. The account used is a generic TNC email address. Individuals can be provided access to monitor cameras (using their TNC email addresses), but this access has more limited functionality.
  - TNC has a free NFP Canva for Teams license that allows TNC staff and volunteers to work collaboratively. Each user is invited into the TNC Team, using their TNC email address.
- There must be at least two people with access to a generic TNC email address to ensure timely responses.

Principle 2: TNC electronic media and associated tools must be protected

Specifically, this means:

- Abiding by the Cyber Security policy
- Physically securing associated tools when not in use
- Recording all associated tools in the Asset Register
- The use of USB storage devices is forbidden.

Principle 3: Use of personal devices must comply with TNC requirements

Staff and volunteers may use personal devices to access TNC electronic media only where approved and where use complies with TNC policies.

Specifically, this means:

- Access to TNC electronic media must occur using TNC-issued accounts only

- Personal email accounts, personal cloud storage and unauthorised applications must not be used for TNC business
- Personal devices used to access TNC systems must comply with the Cybersecurity Policy
- TNC data must not be stored on personal devices outside approved systems
- Approval to use a personal device may be withdrawn at any time if risks are identified.

Principle 4: Electronic media and associated tools are provided primarily for work-related purposes

TNC provides electronic media and associated tools to enable staff and volunteers to work productively. However, it is acknowledged that there are times when limited personal use is acceptable.

Limited personal use:

- Is infrequent and brief
- Does not interfere with the duties of the staff or volunteer and/or or their colleagues
- Does not interfere with the operation of TNC
- Does not compromise the security of TNC or of its systems
- Does not compromise the reputation or public image of TNC
- Does not impact on the electronic storage capacity of TNC
- Does not decrease network performance (e.g. large email attachments can decrease system performance and potentially cause system outages)
- Conforms to the practices for file management and storage of TNC
- Incurs no additional expense for TNC
- Violates no laws
- Does not compromise any of the confidentiality requirements of TNC.

Examples of what would be considered reasonable personal use are:

- Conducting a brief online banking transaction, or paying a bill
- Checking social media during lunchtime
- Sending a brief personal email or text or making a brief personal phone call.

Principle 5: Electronic media and associated tools must not be used in ways that are unacceptable

Electronic media and associated tools must not be used to:

- Create or exchange messages that are offensive, harassing, obscene or threatening
- Visit websites containing objectionable (including pornographic) or criminal material
- Exchange any confidential or sensitive information held by TNC (unless in the authorised course of their duties)
- Create, store or exchange information in violation of copyright laws (including the uploading or downloading of commercial software, games, music or movies)
- Undertake internet-enabled gambling or gaming activities
- Conduct a business or side-project
- Conduct any illegal activities
- Conduct any activities that are not in line with TNC's values
- Create or exchange advertisements, solicitations, chain letters or other unsolicited or bulk email
- Play games.

Principle 6: TNC provides appropriate training and support for provided electronic media and associated tools

Staff and volunteers who use electronic media and associated tools to perform their duties will be trained and able to access support to assist them in working productively and accurately.

4. Roles and Responsibilities

4.1. Overview

Clear roles and responsibilities ensure that TNC policies are implemented effectively, monitored appropriately and aligned with governance expectations.

Accountability for policy application is shared across the organisation, with oversight provided by the designated committee identified in the Policy Information section.

The roles below outline who is responsible for complying with, implementing, and monitoring this policy. Specific responsibilities are clarified further through the RACI table.

4.2. RACI

This RACI identifies who is **Responsible (R)**, **Accountable (A)**, **Consulted (C)** and **Informed (I)** for the activities required under this policy.

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Generic Policy Activities					
Understand and comply with the policy	I	I	C	R	R
Implement policy requirements in daily operations	I	I	A	R	R
Maintain procedures and records required by the policy	I	I	A	R	R
Monitor compliance and identify issues	I	A	R	R	R
Report incidents, risks or non-compliance	I	C	A	R	R
Review policy effectiveness and recommend improvements	I	A	A	C	I
Approve policy revisions	A	C	R	I	I
Policy Specific Activities					
Approve and revoke use of personal devices (BYOD)	I	C	A	C	I
Ensure electronic media use complies with Cybersecurity Policy	I	C	A	R	R
Manage onboarding and removal of TNC electronic media access	I	C	A	R	I

5. Policy Guidelines

The policy guidelines outline the rules, expectations and minimum requirements that must be followed under this policy. These guidelines apply to all individuals covered in the Scope section and support consistent, safe and compliant delivery of TNC operations. Policy-specific guidelines are listed below.

5.1. Electronic media use

- Electronic media must be used in a manner that is consistent with this policy, the Cybersecurity Policy and TNC's values at all times.

6. Processes

The processes describe how the requirements of this policy are applied in practice. They outline the key steps, actions and records needed to implement the policy effectively. Detailed procedures or work instructions, where required, are maintained separately and referenced from this section.

6.1. Access and use of electronic media

Access to TNC electronic media is managed through onboarding, role change and offboarding processes to ensure appropriate authorisation and timely removal of access.

6.2. Recordkeeping Requirements

Records created under this policy must be stored in accordance with TNC's records management requirements. This includes ensuring records are complete, accurate, accessible to authorised personnel, and retained for the required period.

Records may include:

- Security Risk Assessments
- Access approvals or revocations.