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 – INFORMATION TECHNOLOGY & ELECTRONIC MEDIA

1. Policy Information

Title:	Information Technology & Electronic Media
Effective Date:	19-Jan-2026
Policy Owner:	EO
Oversight:	R&CC
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
Associated Tools	Refers to technology required to access Electronic Media such as: • Computers • Phones • POS devices • Tablets.
Cybersecurity Incident	An event that compromises, is suspected of compromising, or attempts to compromise the confidentiality, integrity or availability of TNC systems, data or accounts.
Electronic Media	Includes, but is not limited to: • Email • Instant messaging and chat facilities (e.g. MS Teams) • Internet • Online discussion groups • SharePoint.
IT Support Provider	The external vendor or provider engaged by TNC to deliver technical support, monitoring and cybersecurity services.
Multi-Factor Authentication (MFA)	A security control requiring more than one method to verify identity when accessing systems.
Patch	A software update that fixes security vulnerabilities or other issues in applications or operating systems.
RBAC	Role-Based Access Control, where access permissions are based on job role and restricted to the minimum required for duties.

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.

This policy forms part of TNC's risk and governance system and supports the ongoing protection of TNC's systems, devices, accounts and data from cybersecurity threats and misuse of information and electronic media.

This policy must be read in conjunction with the Risk Management Policy, the Incident Management Policy, and the Records Management Procedure.

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

1.3. Related Documents

- Risk Management Policy
- Incident Management Policy
- Privacy and Data Protection Policy
- Records Management Procedure
- Asset Register
- Cybersecurity Incident Response Plan
- Code of Conduct

1.4. Change Control

Effective Date	Author	Approver	Comments
12-Dec-2023	Bronwyn Evans	BoM	Initial document
08-Apr-2024	Bronwyn Evans	BoM	Updates arising from Loyal IT review of policy
09-Dec-2024	Donna Tudman	BoM	Annual review and minor refinements to RACI
08-Dec-2025	Bronwyn Evans	BoM	• Applied new template • CM ➔ EO • Removed measurement criteria
19-Jan-2026	Bronwyn Evans	BoM	• Introduced explicit BYOD controls to reduce cyber risk associated with personal devices accessing TNC systems and data. • Merged Cybersecurity and Electronic Media policies into a single Information, Technology & Electronic Media policy. Consolidated acceptable use, BYOD and access controls.

1.5. Contents

1. Policy Information 1
   - 1.1. Definitions 1
   - 1.2. Context 2
   - 1.3. Related Documents 2
   - 1.4. Change Control 2
   - 1.5. Contents 3

2. Policy Overview 4
   - 2.1. Purpose 4
   - 2.2. Overview 4
   - 2.3. Scope 4

3. Policy Principles 6
   - Principle 1: Information security is a shared responsibility 6
   - Principle 2: Use of information and technology is a privilege, not a right 6
   - Principle 3: Access is controlled based on role and minimum necessary permissions 6
   - Principle 4: Strong authentication and secure systems protect information and services 6
   - Principle 5: Electronic media must be used appropriately, lawfully and respectfully 6
   - Principle 6: Electronic media and technology are provided primarily for work-related purposes 6
   - Principle 7: Data must be handled securely throughout its lifecycle 6
   - Principle 8: Incidents, risks and concerns must be reported promptly 6
   - Principle 9: Access must be removed promptly when no longer required 6
   - Principle 10: Continuous monitoring and improvement are essential 6

4. Roles and Responsibilities 7
   - 4.1. Overview 7
   - 4.2. RACI 7

5. Policy Guidelines 9
   - 5.1. Acceptable Use of Electronic Media 9
   - 5.2. Personal Devices (Bring Your Own Device – BYOD) 10
   - 5.3. Prohibited Storage Media and Technologies 10

6. Processes 11
   - 6.1. Information and Technology Processes 11
   - 6.2. Recordkeeping Requirements 12

2. Policy Overview

2.1. Purpose

This policy establishes TNC's approach to the secure, responsible and acceptable use of information, technology and electronic media.

It sets out the minimum requirements for:

- protecting TNC systems, devices, accounts and data from cybersecurity threats
- ensuring electronic media and technology are used appropriately, lawfully and in accordance with TNC's values
- safeguarding the confidentiality, integrity and availability of information
- supporting continuity of operations, compliance and organisational reputation.

This policy applies to both the technical security of TNC's digital environment and the way staff, volunteers and others use electronic media and technology when undertaking TNC activities.

2.2. Overview

TNC relies on information technology and electronic media to deliver programs, manage information, communicate with stakeholders and meet governance, funding and compliance obligations.

Cybersecurity threats, inappropriate use of electronic media, or misuse of technology can compromise the confidentiality, integrity and availability of TNC systems and data, expose individuals to harm, damage TNC's reputation and disrupt service delivery.

TNC adopts a layered approach to managing information and technology risks, incorporating preventative, detective and responsive controls. Core requirements include strong authentication, role-based access control, secure devices, patching, monitoring, backups, incident reporting and appropriate use standards.

Electronic media and associated tools are provided primarily for work-related purposes. Limited personal use may be permitted, provided it is reasonable, lawful, does not interfere with duties, does not compromise security, and does not adversely impact TNC, its people or its reputation.

The EO, supported by the IT support provider, is responsible for maintaining TNC's information and technology environment, monitoring risks, and ensuring systems, devices and accounts are protected to an appropriate standard. Staff and volunteers must use systems responsibly, protect credentials and devices, comply with acceptable use requirements and report concerns promptly.

This policy must be read in conjunction with the Risk Management Policy and the Incident Management Policy.

2.3. Scope

This policy applies to all:

- staff
- volunteers
- contractors
- students
- Board members
- any other individuals engaged in TNC activities.

It applies to all:

- TNC-owned or managed devices (computers, tablets, phones, printers, network equipment)
- cloud services and online applications used by TNC
- email, messaging and collaboration systems
- digital accounts assigned to staff or volunteers
- data created, stored, transmitted or processed using TNC systems
- approved personal devices used to access TNC systems or electronic media.

This policy governs both:

- the acceptable use of information, technology and electronic media
- the security and protection of systems, devices, accounts and data.

Policy-specific scope considerations include:

- account management, authentication and access control
- acceptable and unacceptable use of electronic media
- use of personal devices (BYOD)
- device security, patching and monitoring
- cybersecurity incident detection, reporting and response.

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: Information security is a shared responsibility

Everyone who uses TNC systems, devices, accounts or data is responsible for protecting information and contributing to a secure digital environment. Cybersecurity and appropriate use are not solely technical matters and rely on responsible behaviour by all users.

Principle 2: Use of information and technology is a privilege, not a right

Access to TNC systems and electronic media is provided to support TNC activities and service delivery. Access may be limited, monitored or withdrawn where risks are identified or where use does not comply with this policy.

Principle 3: Access is controlled based on role and minimum necessary permissions

Access to systems, data and electronic media must be granted based on role and restricted to the minimum level required to perform duties. Role-based access control (RBAC) supports security, accountability and effective governance.

Principle 4: Strong authentication and secure systems protect information and services

Appropriate authentication, secure devices, patching, monitoring and other technical controls are essential to protect the confidentiality, integrity and availability of TNC information and systems.

Principle 5: Electronic media must be used appropriately, lawfully and respectfully

Electronic media and associated tools must be used in a manner that is lawful, professional and consistent with TNC's values. Use must not expose TNC, its people or the community to harm, reputational damage or legal risk.

Principle 6: Electronic media and technology are provided primarily for work-related purposes

Electronic media and technology are provided to support TNC operations and service delivery. Limited personal use may be permitted where it is reasonable, does not interfere with duties, does not compromise security and does not adversely impact TNC.

Principle 7: Data must be handled securely throughout its lifecycle

Information must be created, stored, transmitted and disposed of securely and in accordance with privacy, records management and other applicable requirements.

Principle 8: Incidents, risks and concerns must be reported promptly

Actual or suspected cybersecurity incidents, misuse of electronic media, or other information and technology risks must be reported as soon as possible to enable timely response and minimise harm.

Principle 9: Access must be removed promptly when no longer required

Onboarding, role changes and offboarding processes must ensure that access to systems, accounts and electronic media is granted appropriately and revoked promptly when no longer required.

Principle 10: Continuous monitoring and improvement are essential

Information and technology risks, incidents and controls must be monitored, reviewed and used to inform ongoing improvements to TNC's information security and acceptable use practices.

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.

Effective management of information and technology risks requires:

- consistent application of security and acceptable use requirements
- responsible behaviour by users of electronic media and systems
- timely reporting and response to incidents and concerns.

The EO is responsible for ensuring that systems, devices, applications and electronic media used by TNC are secure, fit for purpose and used appropriately. This includes overseeing access management, acceptable use expectations, onboarding and offboarding processes, and monitoring of risks and incidents.

The IT support provider supports the EO by maintaining system configurations, security controls, monitoring, backups, endpoint protection and technical support, and by assisting with investigation and response to cybersecurity incidents.

Program Coordinators and Volunteer Coordinators are responsible for ensuring staff and volunteers understand and comply with this policy and use electronic media and technology in accordance with TNC requirements.

All staff, volunteers and others covered by this policy must:

- use information, technology and electronic media responsibly and appropriately
- protect login credentials and devices
- comply with security and acceptable use requirements
- report incidents, suspected incidents, misuse or concerns promptly.

The Oversighting Committee reviews information and technology risks, incidents and control effectiveness in line with the Risk Management Framework.

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

Activity	BoM	Oversighting Committee	EO	Program / Volunteer Coordinators	Staff and Volunteers
Review policy effectiveness and recommend improvements	I	A	A	C	I
Approve policy revisions	A	C	R	I	I
Policy Specific Activities					
Maintain information and technology security controls and standards	I	C	A	C	R
Manage user accounts, onboarding and offboarding	I	C	A	R	I
Ensure MFA, RBAC and password requirements are enforced	I	C	A	C	R
Implement device security, patching and monitoring	I	C	A	C	R
Store, transmit and dispose of data securely	I	C	R	R	R
Ensure electronic media is used appropriately and lawfully	I	C	A	R	R
Approve and revoke use of personal devices (BYOD)	I	C	A	C	I
Detect, report and respond to information and technology incidents	I	A	R	R	R
Review cyber risks and incidents monthly	I	A	R	C	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.

- All accounts used to access TNC systems or data must be secured with MFA and strong passwords.
- Access must be granted based on RBAC and restricted to the minimum necessary for duties.
- Devices used to access TNC systems or electronic media must be secured through approved configurations, encryption, patching and antivirus protection.
- Personal devices may only be used to access TNC systems or electronic media where explicitly approved and must meet security requirements.
- Systems and applications must be kept up to date, with security patches installed promptly.
- Credentials (passwords, PINs, MFA methods) must be kept confidential and must not be shared.
- Data and information must be stored, transmitted and disposed of securely in accordance with privacy and records management requirements.
- Suspicious emails, messages, links or attachments across any electronic media or communication platform must not be opened and must be reported immediately.
- Cybersecurity incidents and misuse or inappropriate use of electronic media, including suspected attempts, must be reported as soon as possible.
- Information must only be stored in approved locations and must not be downloaded or transferred to insecure storage, personal accounts or unauthorised electronic media.
- Remote access must be used responsibly and only through approved, secure methods.
- All staff, volunteers and contractors must comply with onboarding and offboarding processes to ensure appropriate access control to systems and electronic media.

5.1. Acceptable Use of Electronic Media

Electronic media and associated tools are provided primarily for work-related purposes. Limited personal use may be permitted where it is reasonable, lawful, does not interfere with duties, does not compromise security, and does not adversely impact TNC, its people or its reputation.

Limited personal use:

- is infrequent and brief
- does not interfere with the duties of the staff member or volunteer or their colleagues
- does not interfere with the operation of TNC
- does not compromise the security of TNC systems or data
- does not compromise the reputation or public image of TNC
- does not impact electronic storage capacity or system performance
- incurs no additional cost to TNC
- complies with legal, privacy and confidentiality requirements.

Electronic media and associated tools must not be used to:

- create, store or exchange content that is offensive, harassing, obscene or threatening
- access, create or distribute objectionable or illegal material
- disclose confidential or sensitive information except in the authorised course of duties
- create, store or exchange information in breach of copyright or licensing requirements
- conduct gambling, gaming, side businesses or non-TNC commercial activities
- conduct activities that are unlawful or inconsistent with TNC's values
- create or distribute unsolicited bulk messages, chain letters or advertisements
- install or use unauthorised software, applications or services.

5.2. Personal Devices (Bring Your Own Device – BYOD)

Personal devices (including laptops, tablets and mobile phones) may only be used to access TNC systems, **electronic media**, accounts or data where explicitly approved by the EO.

Where approval is granted, the following minimum requirements apply:

- Access to TNC systems or electronic media must occur only via a TNC-issued account protected by multi-factor authentication
- The device must be secured with a strong password, PIN or biometric lock and be configured to automatically lock when not in use
- The device operating system and applications must be supported, kept up to date and patched promptly
- Endpoint protection (anti-virus / anti-malware) must be installed and active
- TNC data and information must not be stored permanently on personal devices and must only be accessed or stored in approved TNC systems
- Personal email accounts, personal cloud storage and unauthorised applications must not be used for TNC business
- Lost, stolen or compromised devices or electronic media used to access TNC systems must be reported immediately
- TNC may revoke access to systems or electronic media, or require additional controls, where a personal device is assessed as posing unacceptable risk

Approval to use personal devices may be withdrawn at any time.

5.3. Prohibited Storage Media and Technologies

To reduce information security and data loss risks, the following are prohibited unless explicitly approved by the EO for a specific operational purpose:

- use of USB storage devices or removable storage media
- use of unauthorised external hard drives or memory cards
- use of personal or unapproved cloud storage services for TNC information
- transfer of TNC information to unauthorised devices, platforms or accounts.

Any approved exception must be documented, time-limited and subject to appropriate security controls.

6. Processes

The processes describe how the requirements of this policy are applied in practice. They outline the key steps, actions and records required to support the secure and appropriate use of information, technology and electronic media. Detailed procedures or work instructions, where required, are maintained separately and referenced from this section.

6.1. Information and Technology Processes

Account Management

- Create, modify and remove user accounts in accordance with RBAC.
- Assign permissions based on minimum required access for duties.
- Remove all access to systems and electronic media promptly when a person exits TNC or no longer requires access.
- Review access permissions regularly and update as roles or responsibilities change.

Authentication and Passwords

- Enforce multi-factor authentication (MFA) for all systems and electronic media supporting TNC operations.
- Use strong passwords in accordance with system requirements.
- Change credentials promptly if compromise is suspected.

Device and Endpoint Security

- Configure devices to meet approved security settings, including encryption, screen locking, patching and antivirus protection.
- Install operating system and application updates promptly.
- Report missing, stolen or damaged devices immediately.

Data and Information Handling

- Store TNC data and information only in approved locations and systems.
- Encrypt sensitive information where appropriate.
- Dispose of information securely in line with records management requirements.
- Do not download, email or transfer information to unauthorised locations, devices or personal accounts.

Electronic Media and Communications

- Use email, messaging and collaboration platforms responsibly and in accordance with acceptable use requirements.
- Do not open suspicious links or attachments.
- Report phishing attempts, suspicious communications or misuse of electronic media immediately.
- Avoid storing sensitive information in electronic media where it is not required for operational purposes.

Monitoring and Detection

- Maintain monitoring tools to detect suspicious activity, unauthorised access, malware, policy breaches or misuse of electronic media.
- Review logs, alerts and notifications as required.

Incident Reporting and Response

- Report all actual or suspected cybersecurity incidents, misuse of electronic media or information security concerns as soon as possible.
- Record incidents in the Incident Register.
- Respond to incidents in accordance with the Incident Management Policy and the Cybersecurity Incident Response Plan.
- Escalate material incidents through the Risk Management Framework.

Remote Access

- Use only approved and secure methods to access TNC systems and electronic media remotely.
- Ensure devices used for remote access are protected by appropriate security controls.
- Log out of remote sessions fully when access is no longer required.

Third-Party and Vendor Access

- Ensure third parties accessing TNC systems or electronic media comply with appropriate security and acceptable use requirements.
- Grant vendor access only when necessary and revoke access immediately when no longer required.

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:

- account creation, modification and removal records
- access permissions and RBAC updates
- device configuration, patching and maintenance records
- cybersecurity and electronic incident reports and response documentation
- logs or reports generated by monitoring tools
- evidence of training, onboarding or awareness related to information, technology and electronic media
- correspondence with third-party providers regarding security matters.