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 – RECORDS MANAGEMENT

1 Policy Information

Title:	Records Management
Effective Date:	15-Aug-2025
Policy Owner:	Executive Officer
Applies To:	All staff, volunteers
Next Review Date:	Aug-2026, or sooner if required

1.1 Change Control

Effective Date	Author	Approver	Comments
15-Aug-2025	Donna Tudman	BoM	Initial version

1.2 Contents

2 Policy Overview

2.1 Purpose

This policy outlines the process for managing digital business records within the organisation, ensuring compliance with legal and regulatory obligations, and maintaining an effective, secure digital records management system.

Effective records management supports better decision-making, reduces duplication of effort, protects sensitive information, and preserves TNC's organisational memory.

2.2 Scope

This process applies to all digital records, including emails, documents, spreadsheets, database entries, and any other form of digital content created or received by the organisation. All records will be stored within the organisation's SharePoint system.

2.3 Context

At Toukley Neighbourhood Centre (TNC), policies are developed in alignment with the TNC Policy Framework.

TNC Policy documents are developed to:

- Assist TNC to meet the objects of the organisation and manage risk effectively
- Assist TNC staff and volunteers in performing their duties
- Outline how TNC will meet governance expectations
- Provide transparency and clarity to TNC staff and volunteers.

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

2.4 Definitions

Term	Explanation
ACNC	Australian Charities and Not-for-profits Commission
BoM	Board of Management
Digital Records	Any records stored in digital format, including but not limited to emails, word processing documents, PDFs, spreadsheets, presentations, and other electronic files.
Retention Period	The duration for which records are kept before being securely archived or deleted.

3 Policy Principles

Principle 1: TNC manages digital records consistently and efficiently

Consistency ensures that everyone follows the same processes for creating, naming, storing, and maintaining records. This reduces confusion, duplication, and the risk of important information being misplaced. Efficiency minimises time wasted searching for records, supports smooth operations, and ensures that resources are used wisely. Consistency also makes it easier to apply retention schedules and comply with regulations.

Consistency applies across all departments and programs, ensuring records are handled in a uniform way regardless of format or source.

Principle 2: Digital records are managed in compliance with relevant legal and regulatory obligations

TNC has obligations under laws such as the *State Records Act 1998 (NSW)*, *Privacy Act 1988 (Cth)*, and ACNC regulations. Compliance means records are stored, protected, and retained for the required timeframes, and that disposal is done lawfully and securely. Failure to comply can lead to legal penalties, reputational damage, or loss of funding.

Principle 3: Digital records that are no longer required are disposed of using approved secure methods

Unnecessary records can create storage clutter, increase costs, and pose a privacy or security risk if they contain sensitive information. Secure disposal ensures that deleted records cannot be recovered, protecting TNC from data breaches and ensuring compliance with privacy and records laws. This applies to both routine and sensitive information.

Principle 4: Important records are retained in a way that allows easy retrieval for operational and compliance purposes, while ensuring only authorised individuals have access

Some records must be kept for years or even permanently for legal, historical, or operational reasons. Storing them in an organised, accessible way ensures that they can be quickly retrieved for audits, legal requests, reporting, or to inform decision-making. Using logical folder structures, metadata, and SharePoint search features supports this.

Principle 5: Staff and volunteers will receive training on digital records management during induction and at least annually thereafter

Training ensures that everyone understands TNC's records management processes and their individual responsibilities. It reduces errors, improves compliance, and helps maintain data security. Regular refresher sessions keep staff up to date with changes in policy, systems (such as SharePoint), and legal requirements. Well-trained people are the most effective safeguard for TNC's information.

The training should cover topics such as:

- The process for creating, storing, and disposing of digital records in SharePoint.
- Understanding of the retention schedule.
- How to securely delete and archive records in SharePoint.

The Records Management Officer will provide guidance and conduct refresher sessions as needed.

4 Policy Guidelines

4.1 Digital Records Retention Schedule

This schedule outlines the types of digital records maintained by the organisation, their retention periods, and the disposal method once they are no longer needed.

Record Type	Retention Period	Disposition	Notes / Rationale
Governance & Legal Records			
Incorporation documents	Permanent	Archive	• Includes digital copies of the certificate of incorporation and bylaws. • Permanent proof of TNC's legal existence and governance history.
Board meeting minutes	Permanent	Archive	• Archive indefinitely as historical records. • Permanent historical and legal record of governance decisions.
Legal agreements (contracts, leases)	7 years after expiration	Shred/Delete	• Retain digitally for the life of the agreement plus the statute of limitations. • Evidence of obligations, rights, and liabilities during and after the agreement.
Insurance policies	7 years after expiration or claim settlement	Shred/Delete	• Retain digitally for the life of the policy plus claims period. • Proof of coverage and to address any claims made after expiry.
Financial Records			
Tax records (e.g., returns, supporting documents)	7 years from the end of the financial year	Shred/Delete	• Required by ATO for compliance and potential audits.
Accounts payable/receivable	5 years	Shred/Delete	• Can be archived digitally if no outstanding issues. • Evidence of financial transactions and resolution of disputes.
Bank statements	7 years	Shred/Delete	• Support for audits, reconciliations, and financial reporting accuracy.
Payroll records	7 years	Shred/Delete	• Includes payment records, tax, superannuation. • Legal requirement for employee entitlements, superannuation, and tax reporting.
Personnel Records			
Employee records (contracts, job descriptions, appraisals)	7 years after termination	Shred/Delete	• Proof of employment terms and performance history for dispute resolution and compliance.
Training records	5 years after completion	Shred/Delete	• Include digital records of certifications and attendance.

Record Type	Retention Period	Disposition	Notes / Rationale
			• Evidence of mandatory and role-specific training for compliance and safety requirements.
Program & Project Records			
Program plans, evaluations	5 years	Shred/Delete	• Reference for future planning and required evidence for funding bodies.
Client service records (case files, support documents)	7 years after closure	Shred/Delete	• Sensitive information requires secure digital disposal. • Maintain service continuity and meet legal, funding, and privacy obligations.
Operational Records			
Policies and procedures	5 years	Archive/Delete	Retain digitally until superseded or outdated. Evidence of organisational standards and practices at a given time.
Correspondence (non-project specific)	3 years	Shred/Delete	Retain only if deemed significant for future reference. Reference for decisions, commitments, and operational context.
Volunteer Records			
Volunteer applications	2 years after volunteer term ends	Shred/Delete	• Record of recruitment decisions and background checks.
Volunteer timesheets	5 years	Shred/Delete	• Evidence for insurance coverage, audits, and funding acquittals.

4.2 Document Naming Standards

4.2.1 Purpose

To ensure TNC documents are named in a consistent, meaningful, and sortable way, making them easy to identify, retrieve, and manage throughout their lifecycle.

4.2.2 General Rules

1. **Meaningful Names**
   The document name should clearly describe the content or purpose of the document. Avoid vague terms such as “Document1” or “New Policy.”
2. **Consistency Across Similar Documents**
   Use the same format and wording for documents of the same type (e.g., all policies, procedures, forms).
3. **Effective Date Inclusion**
   If a document has a formal effective date, it must be included in the document name in reverse date format (*CCYYMMDD*), e.g. 20250815.
4. **Reverse Date Format**
   Use the format *CCYYMMDD* (e.g., 20250812) so files sort chronologically in folders.
5. **No Special Characters**
   Avoid characters such as / \ : * ? " < > | which can cause file errors. Use hyphens - or underscores _ instead.
6. **Version Control**
   If multiple drafts are in circulation, append the version at the end (e.g., `v01`, `v02`, `Final`). Once approved, remove “Draft” from the file name.
7. **Use of Templates**
   Where a TNC-approved template exists, it must be used when creating a document.
8. **Template Standards**
   Templates are standardised to ensure consistency in layout, headings, and formatting, and make use of Microsoft Word styles for headings, body text, lists, and captions.
   Staff and volunteers must be familiar with how to apply and modify these styles.

4.2.3 Naming Format by Document Type

For Policies:

> Policy - [Policy Title] - [YYYYMMDD]
> Example: Policy - Records Management - 20250815

For Procedures:

> Procedure - [Procedure Title] - [YYYYMMDD]
> Example: Procedure - Client Intake Process - 20250901

For Forms:

> Form - [Form Title] - [YYYYMMDD]
> Example: Form - Volunteer Application - 20250820

For Meeting Minutes:

> Minutes - [Meeting Type] - [YYYYMMDD]
> Example: Minutes - BoM - 20250815

For Reports:

> Report - [Report Title/Period] - [YYYYMMDD]
> Example: Report - Annual Review - 20251231

4.2.3.1 Examples of Good Naming Practice

✅ Policy - Child Safety - 20250815

✅ Report - Financial Summary Q2 - 20250701

✅ Procedure - Emergency Evacuation - 20250630

4.2.3.2 Examples of Poor Naming Practice

❌ Policy1.docx
❌ childsafetyFINAL.doc
❌ July meeting notes

5 Processes

5.1 Responsibilities

Role	Responsibility
Record Owners	Ensure digital records under their management are properly created, stored, and disposed of according to this policy.
Records Management Officer	Oversee the retention schedule, monitor record disposal, and conduct periodic audits.
IT Management	Provide backup records and ensure system integrity for SharePoint storage.
All Staff and Volunteers	Ensure that digital records are stored, accessed, and deleted in compliance with this policy.

5.2 Process Considerations

5.2.1 Creation

- Digital records must be created with sufficient detail to meet business and legal requirements.
- File names should be descriptive and follow an agreed-upon naming convention for easy identification.
- Where possible, use SharePoint's version control to ensure changes are tracked and earlier versions can be restored if needed.
- Metadata such as creation date, record type, and version should be included where possible.

5.2.2 Storage

5.2.2.1 Digital Records Storage

- All digital records will be stored in SharePoint, the organisation's designated digital storage system.
- SharePoint offers secure, cloud-based storage with version control, permissions, and metadata capabilities.

5.2.2.2 Organised Folder Structure

- Records should be organised by department, project, or document type in a logical, hierarchical folder structure within SharePoint to ensure easy retrieval.

5.2.3 Access

- Access to digital records within SharePoint should be restricted based on role-based permissions.
- Only authorised staff members should be able to access sensitive records.
- Regular access audits should be conducted by IT management to ensure compliance with security policies.
- Any suspected or actual unauthorised access to records must be reported immediately in accordance with TNC's Data Breach Response Plan.

5.2.4 Retention and Review

- Records should be reviewed at least annually to ensure they are retained according to the retention schedule.
- This review will be overseen by the Records Management Officer and supported by IT management for system integrity.
- The Records Management Officer will conduct an annual compliance check against the retention schedule, with results reported to the BoM.

5.2.5 Destruction/Archiving

5.2.5.1 Digital Destruction

- Records that are no longer needed for operational or legal purposes should be securely deleted from SharePoint using approved software that ensures complete removal of data.

- For sensitive or confidential information, digital destruction should follow industry best practices for data wiping (e.g., following NIST 800-88 or equivalent industry standards).

5.2.5.2 Digital Archiving

- If a record must be retained for historical or legal purposes but is no longer actively used, it should be archived in SharePoint's secure archive storage, where it will remain accessible if required for future reference.
- Archived records should be labelled with metadata for easy retrieval.

5.2.6 Recording Archived or Destroyed Documentation

Logs should be stored securely in SharePoint or another secure system and retained for a minimum of 2 years to provide an audit trail of all archived or destroyed records.

5.2.6.1 Digital Archive Log

A digital log must be maintained for all records that are archived within SharePoint. This log should include the following details:

- Record type and description
- Date of archiving
- SharePoint storage location
- Retention period
- Responsible staff member
- Any specific instructions for retrieval

5.2.6.2 Digital Destruction Log:

A log should be maintained for all records that are destroyed. This log should include:

- Record type and description
- Date of destruction
- Method of destruction (e.g., file deletion, data wiping software)
- Responsible staff member
- Confirmation that destruction was performed securely and in compliance with the policy

5.2.7 Backup Records:

- IT management will ensure that SharePoint is backed up regularly to prevent data loss due to system failures.
- Backup records will be stored securely and accessible for recovery if needed.

5.2.8 Compliance:

Ensure compliance with relevant legislation, including:

- State Records Act 1998 (NSW): Ensure that records are managed in accordance with retention and disposal schedules.
- Privacy Act 1988 (Cth): Ensure that personal data is handled and stored securely.
- Not-for-Profit Sector Governance (e.g., ACNC Regulations): Ensure that records are managed in line with any governance obligations specific to the not-for-profit sector.