POLICY 1.08
Governance
Records Management
Version: 5 **| Next Review:** November 2030

DISTRICT COUNCIL of TUMBY BAY

1 INTRODUCTION

The District Council of Tumby Bay recognises that effective records management is fundamental to governance, accountability and service delivery.

The *State Records Act 1997* governs the obligations and responsibilities of Councils in relation to the management of official records. Under this Act, the Council has an obligation to maintain official records in its custody in good order and condition. This obligation applies not only to the capture, storage, maintenance and disposal of physical records, but also to records in electronic format.

An official record is defined in section 3 of the State Records Act to mean a record made or received by the Council in the conduct of its business. This means that, because Council Members and staff of the Council variously act as representatives of the Council, any record created, sent, received, forwarded or transmitted by Council staff and/or Council Members in the performance and discharge of their functions and duties may be classified as an official record. However, records that are merely transitory, temporary, personal or private in nature will fall outside the definition of "official records".

Recordkeeping practices, including the use of the Electronic Document and Records Management System (EDRMS, Content Manager), provides staff with timely access to accurate and up-to-date information, which in turn provides staff and the Council with a more efficient and effective working environment. This benefits customers in the provision of timely responses to queries and requests, ensuring the Council's integrity and reputation is maintained.

In addition to its record management obligations under the State Records Act, the Council is obliged to keep adequate records in order to fulfill its responsibilities under other Acts such as the *Freedom of Information Act 1991*, as well as fulfilling legal processes, such as discovery and subpoenas. Records may also be required by Royal Commissions, the Ombudsman, the Courts, auditors and other people or bodies.

2 POLICY OBJECTIVES

The objective of this policy is to outline and direct the practices of the staff, consultants and contractors of the District Council of Tumby Bay in relation to the management of its records. The records resulting from the business activities of the Council will be created, received; captured and managed, and be available and readable for the life of the record, to:

- protect the integrity,
- enhance the efficiency,
- preserve the history, and
- provide a business context of the Council.

3 POLICY SCOPE

This Policy applies to all staff, contractors, and consultants engaged in providing services to the Council, across all business processes and locations. It covers all business activities, including decisions made, actions taken, and interactions with stakeholders. The Policy also applies to all records and information created or received through internal operations and through engagement with residents, ratepayers, clients, other agencies, government departments, and businesses.

4 LEGISLATIVE FRAMEWORK

The Council has an obligation under the *State Records Act 1997, Local Government Act 1999,* and *Freedom of Information Act 1991* and other relevant legislation to create, manage, maintain and provide timely access to information.

Adherence to this Policy will ensure the Council is able to:

- meet its legislative responsibilities,
- provide an efficient and effective working environment,
- provide evidence of business transactions and accountability,
- validate and support its decisions and actions, and
- protect the interests of its staff and clients.

5 RECORDS CREATION

Records created within the conduct of their role at District Council of Tumby Bay are the property of Council and therefore must be managed and cared for in accordance with this Policy, associated policies and legislation.

Records are created where there is a legislative, business, fiscal, stakeholder or risk based requirement to document evidence of a transaction, decision, action or communication. When records are created they must be complete, accurate and meaningful and provide a valid and reliable account in a format and media that is readable and accessible for the life of the record.

6 RECORDS CAPTURE

All Council correspondence must be conducted through the council email account with all electronic records captured and saved to the Electronic Documents Management System.

Records in all formats, including emails, will be captured into the records management system (Content Manager), as soon as practicable after creation or receipt.

Records will not be stored on personal devices, drives (both personal or Network) or Outlook accounts, but captured into Content Manager.

7 MAINTAINING RECORD INTEGRITY

The integrity of the records of the Council will be maintained by ensuring:

- records are current, locatable, unaltered,
- duplicates are controlled,
- versions are managed,

- derogatory or negative opinions regarding a person or group should not be recorded,
- storage is appropriate for the record and its format,
- records are able to be located and are readable for the life of the record,
- additional information regarding an action or decision is recorded, and
- migration and conservation are managed to ensure accessibility and readability for the life of the record.

8 ACCESS TO INFORMATION

Access to information will be controlled in line with the requirements of the Council, both internal access by staff and external access by stakeholders. This includes the protection of personal, confidential and sensitive information from internal and external access, and the proactive disclosure of publicly available information as required.

9 RECORDS RETENTION AND DISPOSAL

Records must only be disposed of in accordance with authorised disposal schedules (General Disposal Schedule 40 and other applicable schedules at the time of disposal), as prescribed by the State Records Act 1997. State Records of South Australia's guidelines and standards must be applied to both the destruction of temporary retention records, and the transfer of custody to State Records of permanent retention records. Penalties apply for the intentional removal, alteration or destruction of a record without authorisation to so.

10 ROLES AND RESPONSIBILITIES

10.1 Chief Executive Officer

The Chief Executive Officer of the District Council of Tumby Bay is responsible under section 99 of the *Local Government Act 1999* to ensure that:

a) records required under this or another Act are properly kept and maintained,

b) appropriate and prompt responses are given to specific requests for information,

c) the authorisation of the alteration and validity of records occurs,

d) the authorisation for the destruction of time expired temporary records occurs, and

e) in absence of the Chief Executive Officer their delegate is the Deputy Chief Executive Officer.

10.2 Governance and Records Management Officer

Responsibility for Council's records management system is assigned to the Governance and Records Management Officer, under the supervision of the Chief Executive Officer. The Governance and Records Management Officer is directly accountable to the Chief Executive Officer.

The role of the Governance and Records Management Officer is to provide a strategic focus for record keeping throughout the Council and responsibility for:

a) ensuring that official records are managed in accordance with the State Records Act,

b) establishing records management policies and procedures for the Council as a whole,

c) establishing corporate standards for record keeping and records management,

d) providing consulting services to Council staff and Council Members,

e) developing corporate electronic records management strategies,

f) working with other managers of information resources to develop coherent information architecture across the Council,

g) working with other accountability stakeholders, including FOI officers and executive management staff, to ensure record keeping systems support organisational and public accountability, and

h) providing Council staff and Council Members with appropriate training and tools to allow them to meet their records managements responsibilities.

10.3 Staff, Consultants and Contractors

It is the responsibility of all staff, contractors and consultants to adhere to this Policy by:

a) creating adequate records that reflect the decisions made and actions taken,

b) capturing records into the records management system Content Manager,

c) protecting records from damage or loss by ensuring they are captured in the appropriate system or stored in the correct environment,

d) not altering, removing, destroying or deleting records without proper authority to do so,

e) ensuring all activity carried out on records is recorded and maintained,

f) ensuring the integrity of the Council is maintained,

g) protecting the privacy of individuals in relation to personal information contained within records, and

h) ensuring all records created and managed in the conduct of business are the property of the Council and form part of the record holdings.

10.4 Elected Members

See Policy 2.19 Records Management (Elected Members).

11 RECORD CREATION

Where there is a business, fiscal, legal or stakeholder requirement for evidence of a transaction, decision, action or communication, a record must be created.

Where appropriate, the business knowledge of staff should be documented, not just committed to memory to assist in business operations and future incumbents in undertaking a role.

A record may be created, received and stored in various formats and media. Records include, but are not limited to, letters, reports, photos, e-mails, plans, agendas, minutes, publications and databases.

Records will be created when:

a) advice is given, as evidence of what was said, including documenting phone and face to face advice,

b) a decision is made, as evidence of what was decided, when and by whom eg. minutes of meetings or file notes,

c) an action or activity has taken place eg. maintenance work undertaken, arrangements for a service,

d) an issue or potential issue or crisis arises, including possible litigation or one that might be subject to media exposure and may have an impact on or embarrass the Council,

e) responding to correspondence, complaints or other communication, including phone response to communication, or

f) there is a legislative requirement to do so.

Records need to be:

g) complete, accurate and meaningful to provide a reliable and valid account of what they document,

h) inviolate (not able to be altered after they are transacted or are the final version), and

i) created as soon as practicable after an event or action to ensure they are a reliable and accurate account of what took place.

For records to be authentic, complete and accurate they need to comprehensively identify:

j) exactly what took place,

k) who decided,

l) who authored it,

m) when an action or decision took place,

n) that it originates from the Council,

o) when it was created and received.

11.1 Version Control

Documents and records will include version identification and revision history to provide an audit trail and evidence of the authorised or official version. This includes identification of the version communicated or sent to stakeholders in the conduct of business.

11.2 Integrity of Information

The public, under the Freedom of Information Act 1991, may access documents and records so it is important that a professional approach be taken in relation to documenting and recording all forms of communication with staff, elected members and customers, actions, transactions, decisions and agreements.

Comments of a personal or derogatory nature should not be documented in or attached to records.

11.3 Digital Record Capture into Content Manager

The official records of the Council will be captured into the EDRMS Content Manager system as soon as practicable after creation or receipt.

To give records context and meaning and ensure that they are accessible over time, their capture into a system is an essential step in the overall management of the evidence of the business of the Council. Capture of records into a system ensures accurate and valid information is able to be accessed when it is required and gives the record a unique identifier to ensure it can be validated. It also protects records from alteration or deletion when there is not proper authority to do so.

Whilst many records are automatically created, captured and managed within business systems (e.g. financial transactions), there are many other records, such as those received by the Council, including e-mails, correspondence, minutes, reports etc., which require capture into the Content Manager system.

It is a record when:

a) the information relates to the business of the Council,

b) it is required to provide evidence to support the business and accountability of Council,

c) it identifies issues or risk, or possible issues or risk for the Council, and

d) it adds value to an existing record.

Ephemeral material does not need to be managed within the Content Manager system.

11.4 Duplicates

It is recommended that the creation of duplicates/copies of records is avoided where possible. Where staff create a copy of a record for personal reference, it must be stamped with a copy stamp and the management and deletion of that copy is the responsibility of the person. It is also their responsibility to refer to the original record to ensure currency of information if referencing a copy to provide advice or make a decision.

All duplicate copies of records will be clearly marked as such to enable identification, suitable management in the future and prevent confusion in relation to the identification of the official, valid original. This also will prevent the need to resource the ongoing maintenance, storage and disposal of duplicates by the Records Management staff and sentencing contractors.

11.5 Storage

Records will be stored in the Content Manager system; within corporate business systems or in an area where they are known to exist, are accessible and are protected from damage or inappropriate access.

All staff should ensure that hard copy files and records are protected whilst in their possession.

The Council's records should not be stored in environments where they could be lost or damaged or there is a possibility of unauthorised access (e.g. at home or in cars).

To facilitate access, protection and migration, corporate or business-related information held in electronic media must either be captured into the Content Manager system, appropriate business system, such as Authority, or stored on the shared directory whichever is appropriate at the time.

All records must be stored:

a) away from known hazards,

b) in an environment that suit their media and format,

c) in a location that is secure, accessible and protected, and

d) where retrieval and access is controlled.

In the event of an unforeseen disaster the vital records of the Council, irrespective of media and format, must be identified, salvaged, repaired and conserved.

11.6 Updating of Records

Records will be updated to reflect the current status, current activity or events to ensure the information they contain remains accurate and current. Records containing information about the same issue or event must be related to each other to provide context and a complete representation of the facts. Records must be created and related when an action is undertaken in relation to a record e.g. a response or phone conversation should be documented as a note in Content Manager.

11.7 Alteration

The alteration of records should not occur after the record is finalised, signed or sent to the recipient. When records are captured into Content Manager, the alteration of records is controlled with revisions controlled automatically by the system. If records are saved to the shared directory or hard drives, alteration cannot be controlled and the validity of the record may be questioned if it is required as evidence in court proceedings. For records to be valid they must be inviolate with an audit trail to prove they have not been inappropriately accessed or altered.

11.8 Migration

To ensure records are protected and are accessible for as long as they are required, they must be migrated to new and enduring formats. Records requiring migration will be identified and monitored by the Records Management staff. The application of authorised disposal schedules (GDS 40) will identify records requiring long term or permanent retention which may require migration depending on what media and format they are in. The capture of electronic records into the Content Manager system will ensure long term retention records are able to be identified for migration across systems.

12 ACCESS

12.1 External Access

Records may contain information that is confidential in nature and should not be divulged to certain parties, including other staff within the Council. Staff must be aware of issues relating to confidentiality and sensitivity when managing, accessing or divulging information either on request from within the Council or from outside.

Whilst the Information Privacy Principles, *Privacy Act 1988* and the National Privacy Principles are not applicable to the Council, the principles should be used as a guide in the collection, storage, use and disclosure of personal information.

Records containing information relating to a person require specific management. Personal information means 'information or an opinion, whether true or not true, (including information or an opinion forming part of a database) relating to a natural person or the affairs of a natural person, whose identity is apparent, or can reasonably be ascertained, from the information or opinion including a photograph or other pictorial representation.

Staff must take care when collecting, storing, using and disclosing personal information relating to individuals and the provisions of the *Freedom of Information Act 1991* must be applied in relation to access to records containing personal information. Relevant personal information must only be used and disclosed for the purpose it was collected for.

Requests by the public or media for access to information that is not already publicly available come under the *Freedom of Information Act 1991* and are managed by the Freedom of Information Accredited Officer.

Where documents and records contain:

a) personal information relating to an individual,

b) commercial-in–confidence information relating to the Council or an organisation the Council is conducting business with,

c) working papers relating to a proposed project, or

d) legal opinions,

clarification must be sought from the relevant manager prior to providing access.

12.2 Internal Access

Sensitive and confidential information should be protected to ensure it is not viewed by those who should not have access to it, including staff who are not involved in that particular business activity. Where required, records in all formats should be stored securely to prevent unauthorised access. If they are captured into the appropriate container in Content Manager, access controls will ensure the records are protected from unauthorised access.

Access controls and security protocols of the Council apply to documents and records at the time of creation, receipt and capture to ensure protection of any confidential, private, sensitive or intellectual property from inappropriate access, usage, disclosure or alteration.

13 COPYRIGHT

Staff should be aware of the provisions of the *Copyright Act of 1968* which is the legal protection for people who express ideas and information in writing, visual images, music and moving images. The Council owns the copyright to any publication it produces, and external parties own the copyright of what they produce.

Permission from the owner of the copyright may be required before any work is reproduced. Copyright generally lasts for the life of the creator plus 70 years and where duration depends on year of publication, it lasts until 70 years after it is first published.

14 DISPOSAL

Under the *State Records Act 1997* it is illegal to dispose of records (destroy or remove) except in accordance with an approved records disposal schedule.

General Disposal Schedule 40 (GDS 40) must be applied to the records of the Council when determining how long records should be retained for or when they can be destroyed.

GDS 40 identifies the retention periods for records based on an appraisal of the records value including their cultural, historical, fiscal, business, social and legal value. Other schedules, such as GDS 32, GDS 16, that add a further layer of retention, may also need to be applied.

Records are either temporary (can be destroyed when their retention period has expired) or permanent (must be transferred to State Records of SA 15 years after creation or when administrative use ceases).

Inactive temporary records should be stored in an appropriate storage environment onsite.

Prior to the destruction of temporary value records, (where the retention period has elapsed) approval must be given by the Chief Executive Officer, the Authoriser of destruction.

All documentation relating to the disposal process must be maintained to validate the legal disposal of records if required. This validation may be required for a *Freedom of Information Act 1991* application or for legal discovery.

Information resources that are not considered to be records and have no ongoing value to the Council (ephemeral material) may be destroyed without applying the disposal schedule or seeking approval.

Care must be taken not to destroy information which has value to the Council, which may result in legal action, embarrassment or penalties to the Council.

If there is any doubt about what material can be destroyed contact Records Management staff.

Under the *State Records Act 1997* section 17, the intentional illegal destruction, damage, alteration or removal of official records could incur penalties of $10,000 or 2 years imprisonment of the individual responsible. Further penalties may be applied.

Documents that contain confidential, personal or sensitive information should not be placed in open bins, but either shredded or placed in confidential waste bins when they are being destroyed.

15 POLICY REVIEW

This Policy will be reviewed every four (4) years. The Council has the right to review this Policy at any time, if considered desirable.

16 AVAILABILITY OF POLICY

This Policy will be available for inspection at the Council's Office during ordinary business hours and via the Council's website, www.tumbybay.sa.gov.au. Copies will also be provided to

the public upon request and upon payment of a fee in accordance with the Council's Schedule of Fees and Charges.

17 FURTHER INFORMATION

File reference	R26/10030
Responsibility	Chief Executive Officer
Version	5
Effective date	14/07/2026
Last revised date	12/03/2019
Minutes reference	18c/72026
Next review date	November 2030
Applicable Legislation	*State Records Act 1997* *Local Government Act 1999* *Freedom of Information Act 1991* *General Disposal Schedule 40*
Related Policies	Policy 2.19 Records Management (Elected Members) Policy 2.20 Social Media
Related Documentation	Freedom of Information Statement

AUTHORITY:

Adopted by Council:	10/10/2011 {Motion 19c/102011}
Reviewed by Council:	10/10/2015 {Motion 7c/112015}
Adopted by Council:	10/01/2017 {Motion 19c/102011}
Adopted by Council:	12/03/2019 {Motion 4c/32019}
Adopted by Council:	14/07/2026 {Motion 18c/72026}

SIGNED: 

……..
Responsible Officer

DATED: 14/07/2026

APPENDIX A – GLOSSARY OF TERMS

Term	Definition
Access	The right, opportunity, means of finding, using, or retrieving information. [AS ISO 15489.1 – 2002]
Capture	Deliberate action that results in the registration of a record into a recordkeeping system. For certain business activities, this action may be designed into electronic systems so that the capture of records is concurrent with the creation of records.
Classification	Systematic identification and arrangement of business activities and / or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system. [AS ISO 15489.1 – 2002] – Council Classification Scheme
The Council	The District Council of Tumby Bay (DCTB)
Council staff	Includes persons employed by the District Council of Tumby Bay, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel who access the Council's information resources as part of their role.
Destruction	Process of eliminating or deleting records, beyond any possible reconstruction.
Disposal	Range of processes associated with implementing appraisal decisions. These include the retention, deletion or destruction of records in or from recordkeeping systems and the transfer of custody of ownership of records.
Disposal Schedule General (GDS)	Formal instrument that defines the retention periods and consequent disposal actions authorised for classes of records that are common to agencies of Government
EDRMS	Electronic Document and Records Management System - An automated system used to manage the creation, use, management and disposal of physical and electronically created records (Content Manager).
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. [AS ISO 15489.1 – 2002]
Records Management	The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations. [AS ISO 15849.1 – 2002]
Recordkeeping	Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.
Recordkeeping System	Information system that captures, manages and provides access to records through time.

Term	Definition
Stakeholder	Resident, ratepayer, client, customer, organisation, other agency, government department or employee/s within the organisation who conducts business with or on behalf of the Council.