

# **POLICY 1.08**

## **Records Management**

### **Administration**



**Version: 3 | Next Review: 2021**

---

#### **Document Control**

Intellectual Property - Info-Osmosis © (not to be distributed externally to other parties)

**Next review date** – December 2021

#### **Relevant Legislation**

*State Records Act 1997*

*Local Government Act 1999*

*Freedom of Information Act 1991*

#### **Relevant Standards**

ISO 15489 Records Management

Adequate Records Management Standard 2013

#### **Related Policies**

Elected Member Records Management Policy

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	3 Years	2021	1 of 12

*Printed copies of this document are uncontrolled, refer to Council's Intranet to verify this is the current version.*

Table of Contents

1	Purpose .....	3
2	Scope .....	3
3	Policy Statement .....	3
3.1	Creation.....	3
3.2	Capture .....	4
3.3	Integrity .....	4
3.4	Access.....	4
3.5	Disposal .....	4
4	Roles and Responsibilities .....	4
4.1	Chief Executive Officer .....	4
4.2	Manager’s Responsibility.....	4
4.3	Records Management Staff .....	5
4.4	Staff, Consultants and Contractors .....	5
5	Policy Description .....	5
5.1	Record Creation .....	5
5.2	Version Control.....	6
5.3	Integrity of Information.....	6
5.4	Capture into a System .....	6
5.5	Duplicates .....	7
5.6	Storage.....	7
5.7	Updating of Records.....	7
5.8	Alteration .....	8
5.9	Migration .....	8
5.10	Access.....	8
5.11	Copyright.....	9
5.12	Disposal .....	9
6	Glossary of Terms.....	11
7	Adoption of Policy .....	13

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	2 of 12

## 1. Purpose

The objective of this policy is to outline and direct the practices of the staff, consultants and contractors of the District Council of Tumbay Bay (DCTB) in relation to the management of its records. Records of DCTB are created and received as a result of internal activities, interaction with residents and ratepayers, clients, other agencies, government departments and businesses.

Recordkeeping practices, including the use of the HP TRIM Electronic Document and Records Management System, will provide staff with timely access to accurate and up to date information, which will in turn provide staff and the DCTB with a more efficient and effective working environment. This will lead to benefits for customers in the provision of timely responses to queries and requests, ensuring DCTB's integrity and reputation is maintained.

The DCTB 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 DCTB 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.

## 2. Scope

This Policy applies to all staff, contractors and consultants providing services, all business processes and all locations of the DCTB. It applies to all records and information created and received in the conduct of business, including those records in the custody of the DCTB.

This Policy applies to all:

- Business functions and activities of the DCTB;
- Records created and stored in all formats; and
- Staff, volunteers, consultants and contractors.

## 3. Policy Statement

The records resulting from the business activities of the DCTB 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 DCTB.

Business activities include decisions made, actions taken and interaction with stakeholders.

### 3.1 Creation

Records will be 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 will be complete, accurate and reliable and be created in a format and media that is readable and accessible for the life of the record.

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	3 of 12

### 3.2 Capture

Records in all formats, including emails, will be captured into the records management system (HP TRIM), as soon as practicable after creation or receipt. The containers will be classified and grouped using the DCTB functional classification scheme. Records will not be stored on personal devices, drives (both personal or Network) or Outlook accounts, but captured into HP TRIM.

### 3.3 Integrity

The integrity of the records of the DCTB 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.

### 3.4 Access

Access to information will be controlled in line with the requirements of the DCTB, 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.

### 3.5 Disposal

Records must only be disposed of in accordance with authorised disposal schedules (General Disposal Schedule 20 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.

## 4. Roles and Responsibilities

### 4.1 Chief Executive Officer

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

- Records required under this or another Act are properly kept and maintained; and
- Appropriate and prompt responses are given to specific requests for information.
- The authorisation of the alteration and validity of records occurs.
- The authorisation for the destruction of time expired temporary records occurs.
- In absence of the Chief Executive Officer his delegate is the Deputy Chief Executive Officer.

### 4.2 Manager's Responsibility

The Chief Executive Officer, Directors and Managers are responsible for the DCTB meeting its records management compliance requirements by ensuring:

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	4 of 12

- Records management policy and procedures are included in induction training.
- Recordkeeping responsibilities are included in job and person specifications and performance reviews.
- Staff adhere to the records management policy and procedures.

#### 4.3 Records Management Staff

- Records Management staff are responsible for the management and maintenance of the records management framework by:
  - Making and implementing recordkeeping decisions such as capture, classification, access, storage and disposal in relation to the records of the DCTB;
  - The development and review of records management policies, procedures and guidelines;
  - Reporting on the recordkeeping program, system (HP TRIM) and practices of staff;
  - Providing advice on the use of the records management system, (HP TRIM), processes to managers and staff.

#### 4.4 Staff, Consultants and Contractors

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

- Creating adequate records that reflect the decisions made and actions taken;
- Capturing records into the records management system HP TRIM
- Protecting records from damage or loss by ensuring they are captured in the appropriate system or stored in the correct environment;
- Not altering, removing, destroying or deleting records without proper authority to do so;
- Ensuring all activity carried out on records is recorded and maintained;
- Ensuring the integrity of the DCTB is maintained;
- Protecting the privacy of individuals in relation to personal information contained within records;
- Ensuring all records created and managed in the conduct of business are the property of the DCTB and form part of the record holdings.

### 5. Policy Description

#### 5.1 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:

1. Advice is given, as evidence of what was said, including documenting phone and face to face advice;
2. A decision is made, as evidence of what was decided, when and by whom eg. minutes of meetings or file notes;

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	5 of 12

3. An action or activity has taken place eg. maintenance work undertaken, arrangements for a service;
4. 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 DCTB;
5. Responding to correspondence, complaints or other communication, including phone response to communication; or
6. There is a legislative requirement to do so.

Records need to be:

1. Complete, accurate and meaningful to provide a reliable and valid account of what they document;
2. Inviolable (not able to be altered after they are transacted or are the final version); and
3. 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:

1. Exactly what took place;
2. Who decided;
3. Who authored it;
4. When an action or decision took place;
5. That it originates from the DCTB;
6. When it was created and received.

## 5.2 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.

## 5.3 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 document and record content and file notes.

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

## 5.4 Capture into a System

The official records of the DCTB will be captured into the HP TRIM 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 DCTB. 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 DCTB, including e-mails, correspondence, minutes, reports etc., which require capture into the HP TRIM system.

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	6 of 12

It is a record when:

1. The information relates to the business of the DCTB;
2. It is required to provide evidence to support the business and accountability of DCTB;
3. It identifies issues or risk, or possible issues or risk for the DCTB; and
4. It adds value to an existing record.

Ephemeral material does not need to be managed within the HP TRIM system.

### **5.5 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.

### **5.6 Storage**

Records will be stored in the HP TRIM 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 DCTB's records should not to 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 HP TRIM system, appropriate business system, such as Authority, or stored on the shared directory whichever is appropriate at the time.

All records must be stored:

1. Away from known hazards;
2. In an environment that suit their media and format;
3. In a location that is secure, accessible and protected; and
4. Where retrieval and access is controlled.

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

### **5.7 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 HP TRIM.

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	7 of 12

---

## 5.8 Alteration

The alteration of records should not occur after the record is finalised, signed or sent to the recipient. If records are captured into the HP TRIM, 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.

## 5.9 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 20) 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 HP TRIM system will ensure long term retention records are able to be identified for migration across systems.

## 5.10 Access

### 5.10.1 External Access

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

Whilst the Information Privacy Principles, *Privacy Act 1988* and the National Privacy Principles are not applicable to the DCTB, 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:

1. Personal information relating to an individual;
2. Commercial-in-confidence information relating to the DCTB or an organisation the DCTB is conducting business with;
3. Working papers relating to a proposed project; or
4. Legal opinions.

Clarification must be sought from the relevant manager prior to providing access.**Internal**

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	8 of 12

---

### 5.10.2 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 HP TRIM, access controls will ensure the records are protected from unauthorised access.

Access controls and security protocols of the DCTB 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.

### 5.11 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 DCTB 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.

### 5.12 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 20 (GDS20) must be applied to the records of the DCTB when determining how long records should be retained for or when they can be destroyed.

GDS20 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 DCTB (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 DCTB, which may result in legal action, embarrassment or penalties to the DCTB.

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

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	9 of 12

---

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.

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	10 of 12

## 6. Glossary of Terms

Term	Definition
<b>Access</b>	The right, opportunity, means of finding, using, or retrieving information. [AS ISO 15489.1 – 2002]
<b>Capture</b>	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.
<b>Classification</b>	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] – DCTB Classification Scheme
<b>DCTB</b>	District Council of Tumby Bay
<b>DCTB staff</b>	Includes persons employed by the DCTB, volunteers, trainees, work experience placements, independent consultants and contractors and other authorised personnel who access the DCTB's information resources as part of their role.
<b>Destruction</b>	Process of eliminating or deleting records, beyond any possible reconstruction.
<b>Disposal</b>	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.
<b>Disposal Schedule General (GDS)</b>	Formal instrument that defines the retention periods and consequent disposal actions authorised for classes of records that are common to agencies of Government
<b>EDRMS</b>	Electronic Document and Records Management System - An automated system used to manage the creation, use, management and disposal of physical and electronically created records (HP TRIM).
<b>Record</b>	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]
<b>Records Management</b>	The discipline and organisational function of managing records to meet operational business needs, accountability requirements and community expectations. [AS ISO 15849.1 – 2002]
<b>Recordkeeping</b>	Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.
<b>Recordkeeping System</b>	Information system that captures, manages and provides access to records through time.
<b>Stakeholder</b>	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.

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	11 of 12

## 7. Policy Adoption

**Strategic Link:**

**Delegation:**

**Documentation:** Nil

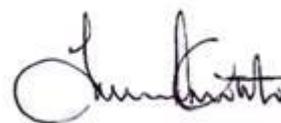
**Authority:** **Adopted by Council:** V1 10/10/2011 {Motion No 19c/102011}

**Reviewed by Council** 10/10/2015 {7c/112015}

**Adopted by Council:** V2 10/01/2017 {Motion No 19c/102011}

**Adopted by Council:** V3 12/03/2019 {Motion No 4c/32019}

SIGNED:



.....  
Responsible Officer

Date: 12 / 03 / 2019

File Reference	Responsibility	Issued	Review Frequency	Next Review	Page
R19/2882	Council	2019	4 Years	2021	12 of 12