

## Guideline to Principle 6: Retain Principle

### A resource for implementing the Standard for Records and Information Governance

#### INTRODUCTION

Records are evidence of business activity. The *Territory Records Act 2002*, (the Act), defines them as 'information created and kept, or received and kept, as evidence and information by a person in accordance with a legal obligation or in the course of conducting business.

Within the context of the Territory Records Act, to be understandable, usable and reliable as evidence of an ACT Government business transaction or event, a record must have the following properties:

1. Content – Text, data, symbols, or images that convey information.
2. Structure – Arrangement of this information into understandable formats, such as designated fields for required information.
3. Context – A direct relationship to the technical and/or business environment that created the record, for example through software applications or metadata.

The Act allows the Director of Territory Records to approve standards for records management, which ACT Government organisations must comply with. The ACT [Standard for Records and Information Governance](#) (the Standard) sets out seven principles that must be applied to ensure that data and information can be managed in ways that allow them to function as records when this is required to support business and accountability requirements. This Guideline is intended to assist organisations to comply with the Retain Principle.

While the term 'record' has a specific meaning, in practice it can at times be difficult to distinguish between records and other types of information or data. The Standard is explicitly designed to meet the requirements of the *Territory Records Act 2002* in terms of records, but is also a guide to good practice approaches for managing information and data for the ACT Government. The [Data Governance and Management Policy Framework](#) is complimentary to the Standard, with the common aim of providing a framework in which information assets can be made, kept and used by the ACT Government.

#### The Retain Principle

The Retain Principle means ACT Government organisations must retain records, information, and data in readily accessible formats by adhering to the retention requirements outlined in

[www.territoryrecords.act.gov.au](http://www.territoryrecords.act.gov.au)

[TRO@act.gov.au](mailto:TRO@act.gov.au)

records disposal schedules.

Importantly, decisions about the retention of records, information and data are guided by the development and implementation of records disposal schedules that provide details on how long records, information and data need to be kept, and if and when they can be nominated for destruction. Records disposal schedules are a by-product of following the Assess Principle.

By adhering to the Retain Principle, ACT Government organisations will ensure their records, information and data are consistently and properly retained in line with business requirements and community expectations and that information assets that are no longer required for government or community purposes can be legally destroyed.

### **Complying with the Retain Principle**

There are three aspects to complying with the Retain Principle:

1. Assessing which records, information and data must be retained in perpetuity.
2. Assessing which records, information and data are eligible for destruction.
3. Ensuring destruction of records, information and data is managed in accordance with the legislative and security requirements.

For an organisation undertaking a comprehensive assessment of their records, information, and data management, use the Territory Records Office's Records Management Maturity Assessment Tool in association with this and other guidelines to implementing the Standard for Records and Information Governance.

### **Further information**

This guideline should not be read in isolation, as the Standard for Records and Information Governance comprises seven separate but inter-related principles. Each principle is supported by its own guideline.

Along with the seven guidelines, further information can be found in the following resources:

- *Territory Records Act 2002*
- International Standard: ISO 15489—Records Management
- ACT Government records disposal schedules
- CARE principles for Indigenous data governance
- Territory Records Office *Records Advice* series

## ASSESSING WHICH RECORDS, INFORMATION AND DATA MUST BE RETAINED IN PERPETUITY

The process of appraisal, which is described further in the [Assess Principle](#), must analyse an organisation's business activities to determine which records, information and data must be kept to meet the organisation's business needs, accountability requirements and community expectations. This analysis involves understanding the significance of the organisation's activities and the recordkeeping requirements that result from them, and the risks to the organisation, the community, or the government of not having access to reliable records, information, and data about those activities. This understanding of the organisation's business activities must also inform decisions about the management of records, information, and data, as set out in the [Protect Principle](#).

The criteria used to identify records, information and data of significance that must be retained as Territory archives are set out in the [Assess Principle](#), and include information assets that are considered essential for the protection and future wellbeing of Australians and their environment, or that have a special capacity to illustrate the impact of government activities on individuals, groups and the environment.

Records identified as Territory Archives as part of the assessment process require particularly careful management to ensure they remain accessible, useable, and understandable in perpetuity. This may include applying additional metadata (see the [Describe Principle](#)), or making particular storage arrangements (see the [Protect Principle](#)).

### Records disposal schedules

Records disposal schedules outline the retention requirements for records, information, and data. They are a by-product of applying the [Assess Principle](#). Records, information, and data of significant and enduring value to the ACT Government and the community are retained as Territory Archives and include:

- significant policies and actions of the ACT Government;
- interaction of the ACT Government with people and their environment; and
- social, political, cultural, and economic development of the Territory as it is influenced by the ACT Government.

Records, information, and data to be retained as Territory Archives must be kept in accessible form and protected – see the [Describe Principle](#), the [Access Principle](#) and [Protect Principle](#) for further guidance.

### Sentencing

Sentencing is the process of applying records disposal schedules to records, information and data. In other words, sentencing is a process for deciding how long records, information or data need to be kept. A records disposal schedule can authorise two main actions in relation to records, information, and data:

[www.territoryrecords.act.gov.au](http://www.territoryrecords.act.gov.au)

[TRO@act.gov.au](mailto:TRO@act.gov.au)

- Retain as Territory Archives: records, information and data that cannot be destroyed due to their enduring value to the Territory and the community; they are to be retained and managed in perpetuity; and
- Destroy: records, information and data that can be destroyed after retention requirements have been met as there is no other business need to keep them.

Destruction of records, information and data is discussed later in this Guideline.

Regardless of whether a decision is to retain or destroy a record, sentencing decisions must be documented within control records such as Electronic Document and Records Management Systems (EDRMS), in file registers or in systems metadata. Documentation of these decisions must include reference to the records disposal schedule and class number applied to the records, and the officer who authorised the decision.

Many ACT Government records are sentenced when they are created by the officer creating or requesting the creation of the record. It is good practice for organisations to have in place quality control mechanisms to monitor the sentencing done by staff when they create records.

Sometimes, particularly with regard to older groups of records, information and data, sentencing will be carried out at some later point in the information asset's life. Where this is the case, sentencing projects should be planned and undertaken regularly (for example, annually) and procedures must be developed to assist with the organisation's consistency of sentencing projects over time – see the Strategy Principle for further guidance. Sentencing projects must be carried out by suitably trained and competent staff, and must be monitored by a qualified records management professional – see the Capability Principle for further guidance.

### **Records about Aboriginal and Torres Strait Islander heritage**

The Act requires organisations to have in place arrangements for preserving records that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage – see the Strategy Principle for further guidance.

A number of categories of records, information and data relating to Aboriginal people and Torres Strait Islander people have been identified that are not authorised for destruction. Organisations must ensure they are aware of the records disposal schedules covering records relating to Aboriginal people and Torres Strait Islander people and take steps to ensure that records, information, and data subject to those schedules are not destroyed.

## **ASSESSING WHICH RECORDS, INFORMATION AND DATA ARE ELIGIBLE FOR DESTRUCTION**

Those records that are not identified as Territory Archives as a result of sentencing may be

destroyed after a specified period. There are two mechanisms for authorising the destruction of Territory Records: through the application of a records disposal schedule, or through a defined and approved 'normal administrative practice'.

### **Records disposal schedules**

Records disposal schedules, a by-product of applying the Assess Principle, determine the minimum retention period for records, information and data of an ACT Government organisation. They outline when records, information and data can be nominated for destruction – see the Assess Principle for further guidance.

Records disposal schedules contain the following elements:

- function name and scope note;
- activity name and scope note; and
- disposal class number and description, and disposal trigger and action.

The disposal trigger and action refers to what can happen to a class of record, information or data source after a nominated period of time.

As discussed above, the process of applying records disposal schedules to records, information and data is known as sentencing. Sentencing activities must be properly planned and authorised by the organisation, be carried out by suitably trained and competent staff, and must be monitored by a qualified records management professional.

### **Normal Administrative Practice**

There is another disposal process that addresses records, information or data sources received or generated that do not qualify for any retention (that is, do not have any business value), known as a Normal Administrative Practice (NAP).

Organisations must define in their Records Management Programs their Normal Administrative Practice for disposing of ephemeral, duplicate or transitory material of no evidentiary or continuing value. See the Strategy Principle for further guidance on developing a Records Management Program. Examples of records that might be destroyed under a normal administrative practice include:

- rough notes, calculations or diagrams used for the creation of records;
- duplicates and copies of documents (which have not been annotated) where the original is retained within the organisation's recordkeeping system;
- facilitative items such as personal emails, appointment diaries or calendars, "with compliments" slips;
- modifications and updating of data as part of the running of established electronic software programs, where such processes do not result in the loss of data of continuing value; and
- published materials used as reference only including pamphlets, leaflets, and brochures.

Normal administrative practice is not intended to replace the use of approved functional records disposal schedules, which are the foremost authority for destruction of organisational records. The Territory Records Office provides guidance on what is an acceptable normal administrative practice, and organisations should take steps to ensure their recordkeeping cultures and staff training reinforce sound recordkeeping and disposal practices.

### **Litigation and Disposal Freezes**

Records disposal schedules state the minimum retention periods for the records, information and data they are applied to. Organisations can choose to retain information assets for longer than stated in the relevant schedule if there is a legal or business need. However, if organisations find that they routinely have need of records for longer than the records disposal schedule requires, this may indicate that a review of the records disposal schedule is needed.

Sometimes unforeseen circumstances arise which require organisations to keep records that in other circumstances might be destroyed. While records disposal schedules generally authorise the destruction of records after a stated period, their destruction is not authorised if the records are required in relation to litigation by or against the ACT Government. Organisations must take reasonable steps to be assured that records, information and data are not subject to legal action before authorising their destruction.

From time-to-time specific issues require a category or group of records, information, and data to be retained that might otherwise have been destroyed. In these circumstances the Director of Territory Records may temporarily suspend the approval of all or part of a records disposal schedule. This is sometimes known as a disposal freeze. Organisations must ensure that they are aware of and have properly considered any disposal freezes before they authorise the destruction of relevant records, information, and data.

### **Other types of disposal**

The term disposal is often interpreted to mean the destruction of records, information, and data. However, the Act also prohibits organisations from transferring the possession or ownership of a Territory record without the approval of the Director of Territory Records. Organisations which outsource any functions, including the management of their records, should seek advice from the Territory Records Office regarding the transfer of their records outside of the Territory's possession.

Ownership of Territory records may be required to be transferred to another entity when Territory enterprises are privatised in part or in full. Organisations should contact the Territory Records Office early in any privatisation process to ensure that the transfer of possession or ownership of records that will be required by the new owners is properly authorised.

## **ENSURING DESTRUCTION OF RECORDS, INFORMATION AND DATA IS MANAGED APPROPRIATELY**

Once records, information and data have been identified for destruction after applying a records disposal schedule class, recording the disposal decisions and calculating the disposal date, the actual destruction must be appropriately approved and securely undertaken.

### **Destruction processes**

Organisations must identify and document procedures for the appropriate approval of decisions to destroy records, information and data after their business use has been exhausted. The process is often referred to as 'destruction concurrence'.

This involves consulting with relevant stakeholders (for example, business owners) to ensure the records, information and data are not needed for legal, business, or other purposes (for example, being subject to freedom of information requests or anticipated litigations or investigations – sometimes referred to as 'holds').

The Territory Records Office recommends the destruction concurrence process be managed with the agreement from the following stakeholders:

- the senior manager of the business unit responsible for the activities documented in the records; and
- the organisation's Records Manager or equivalent.
- The Territory Records Office

It is essential for accountability purposes that an official record is kept of which of the organisation's records have been destroyed and under what authority. This is usually done by annotating a records management database or other records control system with details of the records, information or data that were destroyed, when they were destroyed, the records disposal schedule and the relevant class used, the destruction concurrence process and relevant approvals. See the [Describe Principle](#) for further guidance on retaining data about disposal of records, information, and data.

### **Destruction methods**

The Territory Records Office endorses destruction methods that are:

- authorised (using relevant records disposal schedules and in concurrence with stakeholders);
- documented;
- irreversible;
- secure;
- appropriate for the media and sensitivities of the records, information, or data; and
- as environmentally sound as possible.

Organisations should receive confirmation that destruction has been carried out, including confirmation of the method used. Some destruction methods should be informed by security considerations – see the Protect Principle for further guidance.