GOVERNMENT OF WESTERN AUSTRALIA

Department of **Creative Industries, Tourism and Sport**
State Records Office of Western Australia

Records Management Guideline

Records Retention, Disposal and Destruction

Contents

Purpose

This guideline provides instruction to State organisations on the proper retention, disposal and destruction of their records.

It covers requirements and procedures for conducting a retention and disposal program, as well as appropriate methods of records destruction and media sanitisation.

The guideline is to be consulted when considering records disposal and read alongside the relevant State Records Commission (Commission) Standards and advice issued by the State Records Office (SRO). The matters addressed in this guideline are to be considered and addressed before any disposal – particularly the destruction of records – takes place.

Any Commission Standard or SRO document referred to in this guideline is available on the SRO website.

Background

In accordance with the *State Records Act 2000* (the Act), State organisations are required to maintain a record keeping plan (RKP) that accurately reflects the

organisation's record keeping programs and practices. The retention and disposal of records is an important component of these practices.

Under section 61 of the Act, the Commission, is responsible for establishing principles and standards:

(c) for determining which State records should be State archives; and

(f) for determining the retention periods for State records that are not to be State archives.

Organisations must manage State records in accordance with the retention periods specified in a Commission approved retention and disposal authority (RDA), such as the General Retention and Disposal Authority (GRDA) (for State or Local) Government Information, a Sector Retention and Disposal Authority, or an organisation specific Retention and Disposal Authority.

1 Matters Affecting Records Retention, Disposal and Destruction

1.1 Legislation

The retention and disposal of records is primarily governed by the *State Records Act 2000* (the Act). However, organisations must also consider other legislation relevant to their specific functions and responsibilities, particularly where laws prescribe requirements for how records are created, received or retained. Organisations should also be aware of machinery of government changes, which can alter their functions and legislative requirements. The list of legislation relevant to an organisation are identified in each organisation's RKP.

1.2 Storage of records and archives

State organisations must ensure the usability of records in any format for the full retention period as specified in a RDA. Temporary records must be stored and maintained in accordance with the *State Records Storage - Requirements for Temporary Physical Records.*

Records designated as State archives in an organisation's custody must be maintained in accordance with the *Directions for keeping State archives awaiting transfer to the State Archives Collection.*

Organisations seeking to retain custody of State archives beyond the compulsory transfer period (25 years) must obtain approval from the Commission and maintain compliance with the *Archival Storage Specification.*

1.3 Implementing a regular retention and disposal program

Some benefits of implementing a regular retention and disposal program using an approved RDA includes:

- reduced storage costs
- reduced Freedom of Information (FOI) and litigation exposure
- resource allocation towards records and archives management
- improved information retrieval.

Periodically, RDAs are revised and require organisations to implement the updates. For more information about implementing a revised RDA, please refer to the SRO Records Management Advice- Implementing a revised retention and disposal authority: Resentencing records.

1.4 Extended retention of temporary records

Organisations may decide to retain temporary value records for longer than the stated minimum retention periods set out in an approved RDA due to a required business need.

All State organisations should consider the risk and liability implications of retaining records for longer than legally required, particularly in relation to retention of personal information.

1.5 Personal information

Organisations should ensure records and information that contain personal information are not kept longer than required. State organisations must store personal information securely by:

- not keeping it longer than needed
- protecting it from misuse, unauthorised access, modification or disclosure
- ensuring it is destroyed in a way that prevents any recovery.

For more information, see the SRO Records Management Advice-Retention of Personal Information.

1.6 Information Classification

The Information Classification Policy directs WA public sector agencies to label information according to its sensitivity. The Western Australian Information Classification Policy defines sensitivity as:

“The severity of negative consequences that are likely to result from the release of information. Sensitivity increases in line with the severity of the potential consequences.”

Records containing sensitive or confidential information, where disclosure could harm the organisation or its employees, must be protected with appropriate security measures and destroyed or sanitised using methods that prevent recovery.

1.7 Records formats

Organisations may create, receive and retain records in a variety of formats. The Act does not stipulate or prescribe record formats, it is ‘format free’.

Records must be retained and disposed of according to the information they contain, rather than their format. The only exception is when the format is obsolete or cannot be read. In these cases, even if the information cannot be accessed, the media must still be retained if the RDA includes specific instructions for that format.

Organisations may hold certain formats of records as discrete collections, such as photographs or audio-visual material. Such collections may have additional supporting or contextual information, for example, the records documenting why a photograph was taken and how it was used. Retention and disposal actions of both sets of information should be consistent.

Information held in discrete collections must be identifiable, for example, photographs must be accompanied by information to identify them, such as people, places, events and dates. If this information cannot be located, contact the SRO for advice.

1.8 Digitisation of records

If an organisation intends to digitise physical records and destroy the original source record, they must do so in accordance with the *Specification for Digitisation of State Records* and the *General Disposal Authority for Reproduced Source Records*. For more information, see the SRO Records Management Advice-Digitisation of Paper Records.

1.9 Common Use Contracts (CUAs) and outsourcing

State organisations should be aware of applicable CUAs or contracts that govern records management matters such as storage, retrieval and destruction of paper, digital records or ICT equipment that has a data storage media component.

Before outsourcing the disposal of ICT equipment containing data storage media, State organisations must conduct a risk assessment to ensure the contractor’s disposal procedures comply with these guidelines.

As part of the risk management processes, organisations should evaluate whether it is appropriate to outsource media sanitisation to a contractor, or to carry out sanitisation internally before sending equipment for disposal.

1.10 Disposal Freezes

Disposal freezes may be issued by the State Archivist and Executive Director State Records Office (Executive Director) to stop the destruction of certain records. Any records subject to a disposal freeze, where held by State organisations or their outsourced agents, must not be destroyed regardless of the retention period under the relevant RDA. The records must be retained until the freeze is lifted, as advised by the Executive Director. Information about current disposal freezes is found on the SRO website.

1.11 Freedom of Information (FOI)

The *Freedom of Information Act 1992* (FOI Act) prescribes rights and processes for access to documents held by State organisations. If a request for access under the FOI Act has been lodged, all records relevant to the request must be identified and preserved until the request and any subsequent reviews (including those by the Information Commissioner or the Supreme Court) are completed. This applies regardless of whether the records in question are due for destruction.

When a request involves State archives, copies of the records must be retained with the FOI documentation.

1.12 Investigations, Inquiries, Litigation and Royal Commissions

If any of the above are in progress, likely or imminent, all relevant records must be identified and preserved until all actions are completed. This applies regardless of whether the records in question are due for destruction.

1.13 Legal Deposit

The *Legal Deposit Act 2012* and the associated *Legal Deposit Regulations 2013* support the preservation of Western Australia's published documentary heritage by requiring State organisations to deposit copies of certain published materials with the State Librarian.

The *Premier's Circular No 2025/10: Requirements for Western Australian Government Publications and Library Collections* outlines additional requirements and information for public sector agencies and statutory authorities.

Once relevant publications have been lodged in accordance with legal deposit requirements, remaining copies may be destroyed by the organisation when reference use ceases.

Further information on State organisations' legal deposit obligations is available on the State Library of Western Australia website.

1.14 Records relating to Aboriginal Peoples

Section 76 of the Act requires that retention, disposal and access decisions for certain records about Aboriginal cultural material or heritage must be made in consultation with Aboriginal bodies concerned with the information in the records.

This requirement applies if organisations:

- are directly involved in the discovery and / or management of Aboriginal sites or cultural material, or
- are directly involved with matters relating to the heritage of Aboriginal peoples, or
- hold original records about such matters.

Organisations may contact the SRO for further guidance if they consider that they hold records falling under any of these categories.

1.15 Health records relating to Aboriginal Peoples

As outlined in the *General Retention and Disposal Authority for Local Government Information,* health care facilities must permanently retain the patient records of Aboriginal clients born in 1970 or earlier. In addition, records relating to Aboriginal patients that are created by remote clinics in the Kimberley, Pilbara, Goldfields and Midwest Health regions must also be retained indefinitely.

1.16 Risk management

State organisations should conduct a risk analysis to mitigate the risks of unauthorised destruction or deletion of records, or the use of unsuitable methods of destruction, before the development and implementation of a retention and disposal program.

1.17 Damage to or loss of State records and archives

Records may have been damaged beyond recovery due to disasters such as fire, flood, mould and pest damage, and require destruction before reaching their minimum retention period. In such cases the Commission must approve authorised disposal to occur.

Organisations can self-report to the SRO any damage to or loss of State records via the Reporting Damage to or Loss of State Records webpage.

All State organisations are required to have a Records Disaster Management Plan to ensure they have measures in place to reduce damage to or loss of records from flood, fire, obsolescence of hardware or software, or other circumstances. For more information, see the SRO Records Management Advice-Records Disaster Management Plans.

2 Developing a Retention, Disposal and Destruction Procedure

2.1 Authorisation

Disposal of records and information must be in accordance with an approved RDA and must be authorised.

Details of records to be destroyed or retained as State archives must be reviewed by officer/s with knowledge of the subject matter and authorised for destruction or retention by the organisation's accountable authority, principal officer, or authorised delegate.

2.2 Documentation requirements

Documentation of the authorised disposal of records must be kept by an organisation as evidence of approved disposal decisions or destruction. Details such as record identifiers, relevant RDA, disposal action, date of destruction, destruction method and authorisation should be kept in an organisation's record keeping system or business information system, in accordance with the GRDA.

Where destruction is performed by an outsourced contractor, certificates of destruction or equivalent should be provided by the contractor to the organisation as evidence of secure destruction.

2.3 Records with differing retention periods

Where files contain records with differing retention periods, the complete file must be retained for the longest retention period stated in an approved RDA. In instances where temporary value and archival value information is kept on the same file, the entire file must be retained as a State archive.

In hard copy files, individual pages/documents must not be culled (removed) from files.

2.4 Significance of records and information

In RDAs, each activity is assigned one disposal action, for example, "Retain as State archives" OR "Destroy". Where an activity contains records of both archival (required permanently) and non-archival (temporary) value, two options for disposal action will be provided:

- "Significant"- used to identify records of archival value
- "Other"- used to identify records of non-archival value

The introduction section in the RDA will contain the criteria for identifying which records are "Significant".

The value of the information in records can change over time. When assessing records that are due for destruction, organisations should consider whether they may warrant further retention due to ongoing business or historical value. Contact the SRO for advice if records appear to be of interest as State archives.

2.5 Migration

Before decommissioning any media or systems, organisations should confirm that all data requiring retention has been successfully migrated to the appropriate record keeping or business information system to prevent accidental loss of information. State organisations should ensure they have a migration policy and procedures in place, and conduct a risk assessment, before attempting to migrate records from one system to another.

3 Methods of Destruction

Before conducting disposal, State organisations must ensure all records, including any copies, have been located and are securely destroyed. It is important to check records held in back-ups, cloud storage, with contractors or in offsite storage.

3.1 Sanitisation of Digital Media

ICT equipment, such as scanners, photocopiers, or multi-functional devices, may contain confidential or sensitive information. Before disposing of this equipment, it must be properly sanitised whether undertaken in-house by the organisation or in partnership with an approved CUA contractor. If storage media within the ICT equipment cannot be removed or sanitised, the equipment should be destroyed in a manner that ensures the media is no longer recoverable. Common sanitisation techniques include clearing/overwriting, degaussing, physical destruction and purging.

3.1.1 Clearing/overwriting

This method involves a process of overwriting patterns of data across the entire media to ensure that data stored on it has been replaced with new meaningless data.

3.1.2 Degaussing

Degaussing is the application of a strong magnetic field to magnetic media to randomise the patterns of data on the media. Commercial degaussing units can be purchased to perform this function. Data may potentially be retrievable via this method depending on the degausser used.

3.1.3 Purging

Purging is the process of randomising data so that it is no longer readable and cannot be reconstructed from digital media.

Table of Media and Sanitisation Methods

Media Type	Highly Sensitive	Moderately Sensitive	Non-sensitive
Hard disk drives and magnetic media	Physical destruction	Degaussing Purging Physical destruction	Overwriting Degaussing Purging Physical Destruction
Tapes	Physical destruction	Degaussing Physical Destruction	Overwriting Degaussing Physical Destruction
Optical media-CDs and DVDs	Physical destruction	Physical destruction	Physical destruction
USB / removable media and Memory cards	Physical destruction	Overwriting Physical Destruction	Overwriting Physical Destruction
Mobile Devices (including smart phones)	Physical destruction	Physical Destruction Purging (Refer to device manual for more detailed information)	Physical Destruction Purging (Refer to device manual for more detailed information)
Solid State drives	Physical Destruction	Overwriting Purging Physical Destruction	Overwriting Purging Physical Destruction

Media Type	Highly Sensitive	Moderately Sensitive	Non-sensitive
Hybrid devices	Each component as per its type listed above.	Each component as per its type listed above.	Each component as per its type listed above.

Where sanitisation has failed or the media is unreadable or faulty, use a physical destruction method, such as:

- Incineration
- Melting
- Pulverisation
- Cutting or crushing

When destroying storage media by physical means, organisations should use appropriate equipment to ensure the data stored on the media is irretrievable.

3.2 Shredding

Use for paper, photographs, microform, film or tape. Cross shredding should be used for sensitive/confidential documents otherwise they could be reassembled and reread.

3.3 Pulping

Pulping of shredded paper ensures sensitive and confidential information cannot be reconstructed. Pulping involves mixing paper with water and chemicals, which breaks it down into a fibrous mass.

3.4 Microform and tape records

If records are stored on media such as microform, film or tape (audio or video), the medium should be physically destroyed, or the information overwritten, so that no information is retrievable. Shredding, cutting or chemical recycling are appropriate destruction methods for such media.

4 Unacceptable Destruction Methods

Records require secure destruction to avoid the potential for unauthorised access and information sharing. The following methods are not appropriate for the secure destruction of State records.

4.1 Deletion

Deleting information from media such as hard drives or USBs does not permanently remove records. Recovery software can be used on various media including hard drives and USBs to recover deleted data.

4.2 Burning

Burning is not a recommended destruction method and should only be considered if there are no other destruction facilities available, such as in remote or regional areas. Records should only be burned in accordance with appropriate environmental guidelines and local burning restrictions. Organisations should employ appropriate processes (such as use of incinerators) to ensure that records are completely destroyed.

4.3 Burying and dumping

Records that have been buried or dumped (such as into a skip) can easily be retrieved, creating security risks including unauthorised access and information sharing. These records remain intact and can reveal sensitive and confidential information about the organisation and its employees.

Burying of records is NOT an acceptable destruction method under any circumstances.