State Records Office Guideline

Records Retention, Disposal and Destruction

An Information Management Guideline
for State organisations

January 2024

PURPOSE

The purpose of this guideline is to provide instruction to State organisations in the proper retention and disposal of their records and to ensure that information stored on digital media and devices has been sanitised appropriately for disposal upon decommissioning.

This guideline is to be consulted whenever any records disposal is being considered or conducted.

This guideline should be read in conjunction with relevant State Records Commission Standards and State Records Office (SRO) advice.

BACKGROUND

Under section 61 of the *State Records Act 2000* (the Act), the State Records Commission (the Commission) is responsible for establishing principles and standards governing record keeping by parliamentary departments and government organisations as defined in the Act, including local government organisations.

In accordance with the Act each State organisation has and operates an approved record keeping plan. The Plan comprises one or more documents which, when assessed as a whole, provides an accurate reflection of the organisation's record keeping program and practices.

SRC Standard 2 – Record Keeping Plans: Principle 5 (Retention and Disposal) requires that all records have a minimum retention period for which they must be kept; and some records have continuing value and are to be kept permanently as State archives.

Retention and Disposal Authorities (RDAs) form the retention and disposal component of a Plan and each organisation is to retain and dispose of its records in accordance with an approved RDA.

This Guideline supersedes the *SRO Guideline – Records Retention and Disposal Instructions* and the *SRO Guideline – Sanitizing of Digital Media and Devices.*

Any SRC Standard or SRO document referred to in this Guideline is available on the SRO website.

Relevant legislation and Standards

SRC Standard 2: Recordkeeping Plans

SRC Standard 3: Appraisal of Records

SRC Standard 4: Restricted Access Archives

SRC Standard 6: Outsourcing

SRC Standard 7: State Archives Retained by Government Organizations

SRC Standard 8: Managing Digital Information

General Disposal Authority for Source Records

Retention and Disposal Authorities approved by the Commission.

DEFINITIONS

Disposal - The ultimate action affecting records once they have reached their designated retention period. Disposal can either take the form of

- **destruction** (physically destroying information that is no longer of value, ensuring that no information is retrievable) or

- **archiving** (permanently retaining records with continuing value).

Sanitisation - the process of destroying data on a memory device by digital means, such as erasing or overwriting, or by physical destruction, to make it permanently unrecoverable.

Retention and Disposal Program - A scheduled and managed set of activities required for the regular sentencing and disposal of records.

A Glossary of Terms is available on the State Records Office website.

The Glossary includes terms defined in the Act, as well as terms defined in the context of their application in State Records Commission (SRC) Standards and State Records Office (SRO) publications.

SCOPE

This guideline applies to all State organisations in Western Australia which includes State and local government organisations, and parliamentary departments.

It is intended to be of use to both records management and information technology practitioners.

It is vital that the matters addressed in this guideline are considered and addressed before any disposal – particularly the destruction of records – takes place.

INSTRUCTIONS

1. Obligations

State organisations must use a current RDA approved by the Commission when carrying out their Retention and Disposal Program. An RDA typically takes the form of a General Retention and Disposal Authority, a Sector Retention and Disposal Authority, or an organisation-specific Retention and Disposal Authority.

State organisations must ensure the usability of records in any format for the full retention period as stipulated in an RDA. All State records, whatever their format, are subject to the provisions of an RDA and are to be sentenced in accordance with the function / activity / subject to which they relate.

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

Where a State organisation has applied via its Plan, under *SRC Standard 7: State Archives Retained by Government Organizations* to retain custody of a State archive beyond the compulsory transfer period (25 years), the organisation must maintain the State archive in accordance with the *Archival Storage Specification*.

If restricted access to State archives is required, an organisation must consult with the SRO and identify the archives that are to be restricted in its RDA, including the reasons for restriction and the period of restriction, for approval by the Commission.

Where an organisation has outlined in its Plan that the reproduced version of a record is intended to stand in place of a source record, and the source record is to be destroyed, they must do so in accordance with the *General Disposal Authority for Source Records* and the *Specification for Digitisation of State Records*.

2. Matters affecting records retention, disposal and destruction

State organisations should be aware of the following matters which may affect retention and disposal of State records.

2.1 Common Use Contracts (CUAs) and Outsourcing

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

State organisations outsourcing the disposal of ICT equipment that has a data storage media component should ensure that the contractor performing the disposal work is performing media sanitisation in accordance with this advice.

Organisations should also assess, as a part of their risk management processes, whether it is appropriate to outsource the sanitisation of media to a third party, or undertake sanitisation internally before sending equipment to a third party for disposal.

2.2 Disposal Freezes

A disposal freeze may be issued by the State Archivist and Executive Director State Records Office (Executive Director) to stop the destruction of certain records. Any records under the direction of a disposal freeze held by State or local governments 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 in relation to current disposal freezes will be made available via the SRO website.

2.3 Freedom of Information

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.

Any FOI requests identified as State archives **must** contain copies of the records that were the subject of the requests.

2.4 Implementing a revised Retention and Disposal Authority (RDA)

When an RDA has been revised and approved by the Commission it will typically supersede / replace the previous relevant RDA. State organisations **must** cease using the previous RDA and use the new RDA to sentence and dispose of records from the date of its approval. Organisations **must** re-sentence relevant records and should refer to the SRO advice *Resentencing records: implementing a revised retention and disposal authority.*

2.5 Investigations, Inquiries, Litigation and Royal Commissions

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

2.6 Legal Deposit

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

Premier's Circular No 2021/14: 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.

2.7 Legislation

The retention and disposal of records falls primarily under the provisions of the Act. However, organisations **must** be aware of other legislation relevant to their functions and responsibilities, particularly where it may prescribe which records are to be created or received by the organisation. Other legislation that addresses record keeping matters should be identified in each organisation's Plan.

2.8 Personal Information

Personal information is defined in the Glossary to the *Freedom of Information Act 1992* as:

"information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead -

> (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or
>
> (b) who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample."

Effective management of personal information (information that identifies an individual or could identify that individual) is of vital importance to all State organisations that are required to obtain personal information about individuals in order to deliver services. Inappropriate use of personal information can compromise an individual's privacy, leading to undesirable outcomes for both the individual and the organisation. (Adapted from: Ombudsman Western Australia, Guidelines for Agencies Management of Personal Information, May 2013.)

State organisations must store personal information securely, keep it no longer than necessary, protect it from misuse, unauthorised access, modification or disclosure, and dispose of it appropriately by ensuring no information is retrievable.

2.9 Record Formats

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

Records **must** be retained and disposed of according to the information they contain, rather than their format, unless a relevant RDA contains specific instructions for a particular format.

Organisations may maintain certain formats of records as discrete collections, such as photographs or audio-visual material. Such collections may have accompanying 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** identify people, places, events and dates. If this information cannot be located, contact the SRO for advice on appropriate disposal.

2.10 Records relating to Aboriginal People

Section 76 of the Act requires that retention, disposal and access decisions for certain records about Aboriginal cultural material or Aboriginal 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 Australians, 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.

Health records relating to Aboriginal people - As outlined in the *General Retention and Disposal Authority for Local Government Information,* health care facilities **must** retain Aboriginal patient records indefinitely for clients with a date of birth prior to and including 1970. In addition, Aboriginal patient records created by remote clinics in the Kimberley, Pilbara, Goldfields and Midwest Health regions **must** also be retained indefinitely.

2.11 Regular disposal and destruction

Records and information should not be kept longer than is necessary. Implementation of a regular Retention and Disposal Program reduces storage costs, allows resources to be allocated towards managing records and information of long term and permanent value; and makes information easier to find.

2.12 Retaining temporary records for longer periods

Organisations may decide to retain temporary value records and information for longer than the stated minimum retention periods set out in an approved RDA due to a required business need. It is not necessary to consult the SRO to do so, however, organisations should document why the longer retention periods were adopted. Organisations should also consider the risk and liability implications if they retain records for longer than legally required, particularly in relation to retention of personal information.

2.13 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.

2.14 Significance of records and information

In RDAs, each activity is assigned one disposal action, for example, "Required as State archives" OR "Destroy". Where an activity contains records of both archival and non-archival value, two disposal actions will be assigned:

- "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.

2.15 Records impacted by a disaster

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 SRO **must** be contacted for authorised disposal to occur.

3. Procedures

3.1. Conducting a Retention and Disposal Program

3.1.1. Responsibility for records retention, disposal and destruction

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.

Documentation requirements

Documentation of the authorised disposal of records and information 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 records management system or other business information system and retained in accordance with the applicable General Retention and Disposal Authority.

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

Security

Organisations must ensure that records and information of temporary value are destroyed securely, in a method appropriate to their format, and in such a way that they cannot be reconstructed. It is important that all copies are located and securely destroyed, including those held on back-ups, cloud storage, or by third-party providers.

Organisations should undertake a risk assessment of records and information contained on various media to determine the sensitivity of the content and the most appropriate method of sanitisation. Negative consequences may result if confidential or sensitive information can still be recovered or is unintentionally released.

Organisations must ensure that information is not inadvertently destroyed when media or systems are decommissioned without data being migrated.

Public sector agencies should refer to the Western Australian Government Information Classification Policy to assess the sensitivity of information and the WA Government Cyber Security Policy regarding managing their cyber security risks.

3.1.2. 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 archived.

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

3.2. Safety Considerations

When using a method of physical destruction it is essential that any relevant occupational health and safety measures are followed. To ensure you are following appropriate measures refer to the relevant Western Australian work health and safety organisation (currently Worksafe) for more information.

3.3. Methods of Destruction

3.3.1. Digital records and memory storage devices/media sanitisation

When State organisations replace or dispose of information stored on media the information must be sanitised to ensure that information stored on it cannot be retrieved or reconstructed.

Organisations are responsible for ensuring that digital records are accessible for the full retention period and for managing the migration process to new platforms whenever these are upgraded. If digital records have archival value, organisations are responsible for maintaining those records so that they will be accessible for all time.

ICT equipment, such as scanners, photocopiers, or multi-functional devices, may contain confidential or sensitive information and sanitisation should be performed by the organisation prior to outsourcing the disposal of the equipment. 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.

The process for sanitising media may vary according to the degree of sensitivity of the information it contains and the type of media used. Methods of sanitisation include clearing/overwriting, degaussing, physical destruction and purging.

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.

Degaussing

Degaussing is the application of a strong magnetic field to magnetic media to randomize 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.

Physical Destruction

The nature of some storage media means that the only reliable method of sanitising is physical destruction. Methods include:

- Disintegration
- Incineration
- Melting
- Pulverisation
- Shredding

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

Purging

Purging is the process of completely erasing obsolete information from digital media through randomising the data so it is unrecoverable.

3.3.2 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
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	Overwriting

		Purging Physical Destruction	Purging Physical Destruction
Hybrid devices	Each component as per its type listed above (eg: magnetic drive and flash media drive)	Each component as per its type listed above (eg: magnetic drive and flash media drive)	Each component as per its type listed above (eg: magnetic drive and flash media drive)

Note: where sanitisation has failed or the media is unreadable or faulty, use a physical destruction method to destroy.

3.3.2. Paper and Physical Records

Paper and physical records must be destroyed via one of the following methods.

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

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.

Pulping

Paper is mixed with water and chemicals to break it down into pulp. Pulping of shredded paper ensures that sensitive information cannot be reconstructed.

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.

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.

REFERENCES

Australian Cyber Security Centre June 2022, *Information Security Manual*, Australian Government, Australian Signals Directorate, viewed 4 Jul 2022, <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/archived-ism-releases >

National Archives of Australia, n.d., Complaint Destruction of Australian Government Information, Australian Government, National Archives of Australia, viewed 4 Jul 2022, <https://www.naa.gov.au/information-management/disposing-information/information-disposal/compliant-destruction-australian-government-information>.

Office of Digital Government, October 2021, *WA Government Cyber Security Policy*, Government of Western Australia, Department of Premier and Cabinet, Office of Digital

Government, viewed on 1 July 2022, https://www.wa.gov.au/system/files/2022-01/WA%20Government%20Cyber%20Security%20Policy.pdf

Public Record Office Victoria, June 2022, Destruction – Information about destroying records, Victoria State Government, Public Record Office Victoria, viewed on 4 July 2022, < https://prov.vic.gov.au/recordkeeping-government/a-z-topics/destruction>.

Public Record Office Victoria updated Jul 2019, *Guideline 3 – Destruction* (Version: 1.2), Victoria State Government, Public Record Office Victoria, viewed on 4 Jul 2022, <https://prov.vic.gov.au/sites/default/files/files/documents/pros_1013_g3_v1.2.pdf>

Queensland Government, updated 11 July 2023, *Disposal advice for records managers*, viewed on 19 Dec 2023, < https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/disposal-of-records/disposal-advice-for-record-managers >

State Records NSW, updated March 2020, *Destruction of records*, NSW Government, State Records NSW, viewed on 19 Dec 2023, <https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/destruction-records#methods-of-destruction>

RELATED DOCUMENTS

Archival Storage Specification

Directions for keeping State archives awaiting transfer to the State Archives Collection.

Glossary of Terms

State Records Office Guideline – Managing Digital Records

State Records Office Guideline - Resentencing Records: implementing a revised retention and disposal authority

Specification for Digitisation of State Records

Active date

January 2024

Review date

January 2026

For further information – please contact the State Records Office at sro@sro.wa.gov.au