



Public Record Office Victoria
PROS 10/13
Disposal

Guideline

3

Destruction

Version Number: 1.0

Issue Date: 09/08/2010

Expiry Date: 09/08/2015

Table of Contents

- 1 Introduction4**
 - 1.1 Public Record Office Victoria Standards4
 - 1.2 Purpose.....4
 - 1.3 Scope.....4
 - 1.4 Related Documents.....5

- 2 Destruction Objectives6**
 - 2.1 Legal6
 - 2.2 Timely.....7
 - 2.3 Authorised.....7
 - 2.4 Secure & Irreversible.....8
 - 2.5 Documented.....8
 - 2.6 Safe.....9
 - 2.7 Environmentally Friendly.....9

- 3 Methods of Destruction10**
 - 3.1 Electronic Media.....10
 - 3.2 Electronic Systems.....10
 - 3.3 Paper.....11
 - 3.4 Film & Microform11
 - 3.5 Inappropriate Methods of Destruction12

- 4 Using a Contractor to Destroy Records13**
 - 4.1 Selecting a Contractor.....13
 - 4.2 Responsibilities13
 - 4.3 Transport of Records13
 - 4.4 Documentation13

- 5 References14**

- Appendix 1: Checklist for Records Destruction.....15**

Copyright Statement

© State of Victoria 2010

This work is copyright. Apart from any use as permitted under the *Copyright Act* 1968, no part may be reproduced through any process without prior written permission from the publisher. Enquiries should be directed to Public Record Office Victoria, PO Box 2100, North Melbourne, Victoria 3051 or email: ask.prov@prov.vic.gov.au.

Disclaimer

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Guideline. This Guideline does not constitute, and should not be read as, a competent legal opinion. Agencies are advised to seek independent legal advice if appropriate.

Acknowledgements

The Public Record Office Victoria would like to acknowledge the valuable contribution of members of the *Disposal Advisory Group* during the development of this Guideline.

1 Introduction

1.1 Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973*, the Keeper of Public Records ('the Keeper') is responsible for the establishment of legally binding Standards for the efficient management of public records and for assisting Victorian government agencies to apply those Standards to records under their control.

Recordkeeping Standards issued by PROV reflect best practice methodology. This includes international Standards issued by the International Organisation for Standardisation (ISO) and Australian Standards (AS) issued by Standards Australia in addition to PROV research into current and future trends.

Heads of government agencies are responsible under section 13b of the *Public Records Act 1973* for carrying out, with the advice and assistance of the Keeper, a programme of efficient management of public records that is in accordance with all Standards issued by the Keeper.

In Victoria, a programme of records management is identified as consisting of the following components:

- A Recordkeeping Framework;
- Recordkeeping Procedures, Processes and Practices;
- Records Management Systems and Structures;
- Personnel and Organisational Structure; and
- Resources, including sufficient budget and facilities.

A programme of records management will cover all an agency's records in all formats, media and systems, including business systems.

1.2 Purpose

The purpose of this Guideline is to provide practical assistance for agencies in the destruction of records when allowed in Disposal Authorities, which includes Retention & Disposal Authorities (RDAs), Single Instance Disposal Authorities (SIDAs) and Normal Administrative Practice (NAP).

This Guideline can be used by both agency staff disposing of records themselves as well as contractors destroying records on behalf of an agency.

1.3 Scope

The destruction of records, both electronic and physical (paper, film, microfilm etc.), is addressed by this Guideline.

1.4 Related Documents

This Guideline supports the *Disposal Standard* (PROS 10/13) and Specification 2 which are supported by a number of other Guidelines as shown in the following relationship diagram:

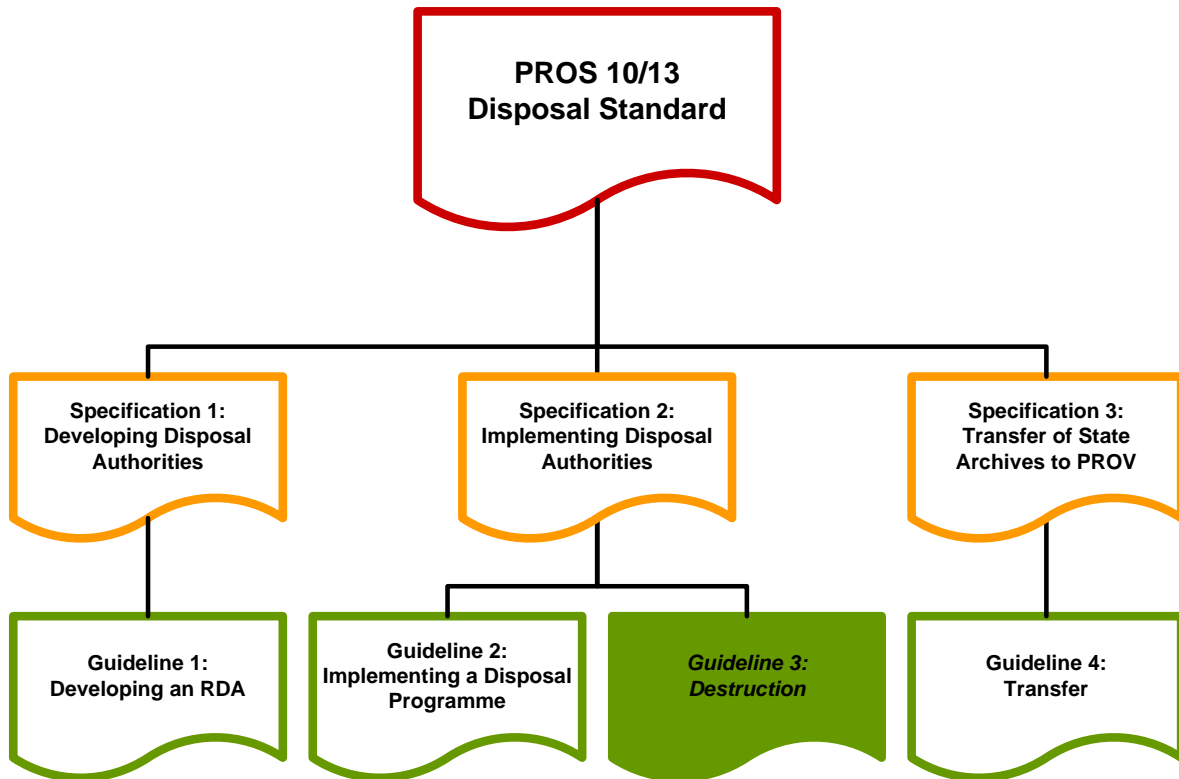


Figure 1: Relationship Diagram

2 Destruction Objectives

“Records Destruction” refers to the rendering of records as unreadable and irretrievable. Public records can only be destroyed or otherwise disposed of in accordance with Standards issued under Section 12 of the *Public Records Act 1973*. The destruction of records should meet the following objectives.

2.1 Legal

The PROV *Disposal Standard* defines three processes that can lead to the legal destruction of records:

- Destruction of records under the principle of Normal Administrative Practice (NAP).
- Destruction of records covered by a Retention & Disposal Authority (RDA).
- Specific authorisation to destroy records not covered by NAP or an existing RDA.

2.1.1 Normal Administrative Practice (NAP)

Public records may be destroyed by a public sector employee without any authorisation from PROV provided that they fall within the category of Normal Administrative Practice (NAP). NAP allows for the disposal of:

- Working documents consisting of rough notes and calculations used only as a means to assist in the preparation of other records such as correspondence, reports and statistical tabulations.
- Drafts not intended for retention as part of the agency’s records, the content of which has been reproduced and incorporated in the agency’s recordkeeping system.
- Additional copies of documents, emails and publications maintained for reference purposes.

The decision to destroy records under NAP is the responsibility of the government agency. The agency is responsible for ensuring that all staff understand NAP and are able to apply it correctly in their day to day work, for instance, in the management of email records.

The following factors should be considered:

- Is there any further administrative need to retain the record?
- Are others still using the record?
- If you believe it’s just a copy, are you sure that an authoritative version has been kept?

2.1.2 Retention & Disposal Authorities (RDAs)

Retention & Disposal Authorities (RDAs) specify the minimum retention periods for classes of records and authorise the destruction of time-expired records.

All RDAs, whether general or specific to a particular agency, do not attempt to describe each particular record type or format, but instead provide a broad description of the functions and activities to which the records relate.

2.1.3 Single Instance Disposal Authorities (SIDA)

To destroy any record not covered by either NAP or an RDA, it is necessary to be issued with a Single Instance Disposal Authority (SIDA) from PROV. These are typically used for:

- Records of functions or activities which are no longer performed by the agency.
- Records inherited by an agency as a result of machinery of government changes (that is, an agency inheriting a function previously undertaken by a different agency).

These were formerly referred to as ad-hoc disposal authorities.

2.2 Timely

Whilst records should not be destroyed while there is still a need for them, it is also important not to keep records longer than necessary. This will minimise storage costs and administrative overheads, comply with privacy requirements and reduce the risk associated with inappropriate information release.

If decisions are made to retain records longer than the minimum retention time, a record of the justifications for the decision should be documented to assist with future disposal.

Records are usually destroyed when they have reached the end of a specified retention period. However, it is necessary to ensure that they are no longer required, prior to their destruction. Timely destruction must therefore be balanced with internal authorisation. With the exception of NAP, records destruction requires the completion of an internal sign off process within the organisation.

2.3 Authorised

2.3.1 Authorisation from Public Record Office Victoria

RDAs are the legal instruments which provide the disposal authorisation upon which a government agency can act. They set a minimum period for retention of the records. A record which is authorised for destruction in an approved and current RDA may be destroyed at the end of the retention period, if it is no longer required by the government agency. See *Guideline 2: Implementing a Disposal Programme* for advice on applying RDAs to records.

From time to time, Public Record Office Victoria may place disposal freezes on groups of records. Records subject to disposal freezes may not be destroyed, regardless of what the current RDA authorises. These records need to be retained by the agency until such time as the freeze is lifted or directives from PROV are received.

2.3.2 Internal Authorisation

RDAs set a minimum period for retention; however it is important to ensure that the government agency has no further business or legal need for the records. This can be achieved by ensuring that appropriate internal authorisations are in place.

Once the requirements for retaining records have been met, an appropriate staff member, for example a senior manager, should give the final internal approval for the records destruction. It is important that a specific person be assigned and be responsible for this process.

2.3.3 Legislative Provisions

Under s. 19 of the Public Records Act, it is an offence to unlawfully destroy a public record. Destruction of a record is unlawful if it is not done in accordance with standards established under section 12 of the Act.

In addition, government agencies should not destroy records that are the subject of a current Freedom of Information (FOI) request until all avenues of appeal have been met.

Agency staff should be aware of the provisions of the *Crimes (Document Destruction) Act 2006* which has created a new offence relating to the destruction of a document or other object that is reasonably likely to be required in evidence of a legal proceeding.

2.4 Secure & Irreversible

Records should always be destroyed securely, with a commensurate level of security that was maintained during the life of the records. Destruction of records should be performed by an officer of the agency or by an authorised contractor (as described in section 4) if destruction has been contracted out.

Sensitive records contain information which, if released, could have a detrimental effect on people or organisations. Information which may be regarded as sensitive can fall into a number of different categories:

- Personal and private information – for example patient health records, employment records.
- Financially or commercially sensitive information – for example tender documentation.
- Information relating to criminal or civil investigations – for example fraud investigation records.
- Information that poses a security risk – for example security procedures.

Extra care should be given to records containing sensitive information. Such mediums as lockable “wheelie” bins may be used for particularly sensitive records. Sensitive records not confined to bins should be transported in totally enclosed and lockable vehicles and destroyed in the presence of an authorised person.

Destruction of records should be irreversible. This means that there is no reasonable risk of the information ever being recovered. Failure to ensure this may lead to unauthorised release of information. Further details on Information Security are available in the Protective Security Manual (PSM)¹ issued by the Australian Government.

2.5 Documented

Destruction of all records must be documented so that the agency is able to ascertain whether destruction has taken place. This applies equally regardless of format (i.e. scanned records, electronic records or paper records). Proof of destruction may be required in litigation proceedings, in response to FOI requests or as requested from PROV.

¹ Attorney-General's Department 2009, *Protective Security Manual (PSM)*, Australian Government, Canberra, viewed 19 March 2010, <[http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual\(PSM2005\)](http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005))>.

Documentation and recordkeeping systems should note the specific RDA and disposal class under which the records are destroyed, along with the date of destruction.

Government agencies should keep a destruction register which links individual records to be destroyed with consignments sent for destruction. Should the destruction be performed by a contractor or service provider, this will strengthen the evidence that records have actually been destroyed. The destruction register should note:

- Title and unique identifier of record
- Relevant RDA and class
- Date of destruction
- Individual authorising destruction and their position in the agency

A certificate of destruction should be generated when records are destroyed. The certificate of destruction should be placed on a file together with any other destruction documentation. The destruction certificate should note:

- Description of records
- Date of destruction
- Method of destruction
- Individual performing/supervising destruction

2.6 Safe

Methods of destruction should always take into consideration the health and safety of the persons undertaking the destruction. If you are unsure whether occupational health and safety is being adequately covered, please contact Worksafe Victoria or the equivalent regulatory authority.

2.7 Environmentally Friendly

In keeping with today's environmental practices, all records should be destroyed in an environmentally friendly manner wherever possible and practicable. Records of all forms should be recycled wherever possible. Extra care should be taken in the destruction of toxic or noxious material, for example by the use of chemical recycling. Agencies are recommended to seek specialist advice from such organisations as the Environmental Protection Authority on this issue.

3 Methods of Destruction

3.1 Electronic Media

Destruction of electronic records is considerably more complicated than paper records because of the variety of media that exist and the continual development of technology. Agencies are recommended to seek advice from PROV, should they need to destroy media which does not fall into the categories below.

3.1.1 Magnetic Media

Records stored on magnetic media, such as tapes and floppy disks, can be bulk erased by subjecting them to a strong magnetic field (degaussing). Degaussing units are available that can be used for this purpose. Magnetic media can then be reformatted and reused. If it contains sensitive information it should be physically destroyed by shredding, corrosion or melting. Note that deletion does not remove data from magnetic media and is therefore insufficient for the destruction of records.

3.1.2 Optical Media

Records held on optical media, for example CDs and DVDs, should be physically destroyed by cutting or crushing.

3.1.3 Hard Drives

Hard drives, such as those in personal computers, servers, mobile devices and USB sticks should be degaussed and reformatted when they are decommissioned. When servers and hard drives containing sensitive information are decommissioned, they should be physically destroyed by shredding, corrosion or melting. If computers and servers are to be reused, they should be degaussed and reformatted. If a drive has contained sensitive information in the past, it should not be downgraded in terms of its security access.

3.2 Electronic Systems

3.2.1 Business Systems

A business system may be a single database, or may be several linked programs and policies which form the necessary infrastructure to support business processes. Records are typically retained within such systems.

Records in business systems should be destroyed using the functions of the system where possible, to maintain system integrity. Deletion is a practical method of destruction within such systems, but is only appropriate where the system is in active use. This is because the creation of new records should ensure that deleted ones are overwritten within a reasonable timeframe.

If the system is not in active use, or contains highly sensitive information, the records should be overwritten rather than just deleted to prevent them from being recovered. Software utilities exist that are able to overwrite data stored by business systems.

The agency should retain a record of destruction within business systems. If the system doesn't automatically record the destruction of records, external tools such as audit logs may be used.

3.2.2 Electronic Document & Records Management Systems (EDRMS)

An Electronic Document & Records Management System (EDRMS) should ensure that, when a record marked for destruction is destroyed, all of its versions and renditions are destroyed. Where the same record appears in more than one file, the record and its renditions should be removed from the file when it is destroyed but should not be finally deleted until all occurrences of the record have been destroyed.

In some environments it is desirable to retain information about records which have been destroyed within an EDRMS. This should include all the metadata relevant to uniquely identify each record. This will allow the agency to be aware of the records it has held and the dates they were destroyed or disposed of, without incurring the overhead of keeping all the detailed record metadata.

3.2.3 Back-up Systems

Copies of records may be held in back-up systems. If a record has been destroyed, copies should be destroyed as well. It may be impractical for some back-up systems to destroy specific records in a back-up. It is possible to wait until the back-up media has been recycled, but back-up cycle times should be taken into consideration. If the cycle time is too long, records within the backup system should be overwritten. It may be necessary to conduct a risk assessment to determine the period of time which is acceptable.

Please refer to *Operations Management Guideline 3* for further information regarding the management of the systems lifecycle.

3.3 Paper

3.3.1 Shredding & Pulping

Security provided by shredding is dependant on how the paper is treated afterward. Shredded paper should be pulped as modern technology allows reconstruction of shredded paper.

3.3.2 Pulping

Pulped paper is reduced to its constituent fibres. If performed correctly, it is a very secure method of destruction. Pulped paper should be recycled to reduce the environmental impact of your agency.

3.4 Film & Microform

Video, cinematographic and microforms (which covers microfilm, microfiche, aperture cards and x-rays) can be destroyed by shredding, cutting, crushing or chemical recycling.

3.5 Inappropriate Methods of Destruction

The following methods do not meet all the destruction objectives outlined in section 3 and should not be used as means of record destruction.

3.5.1 Deletion

Simply deleting records from a hard drive or USB device does not permanently erase them, and they can easily be restored for some time after deletion.

3.5.2 Dumping

Dumping of records does not result in their destruction and security can be easily compromised.

3.5.3 Burying

Records can be uncovered within hours of burying, thus security cannot be assured.

3.5.4 Burning

The burning of records causes unnecessary environmental pollution.

3.5.5 Shredding without Subsequent Pulping

Shredded records (without being pulped) can be reconstructed using new technologies and thus this process is not irreversible.

4 Using a Contractor to Destroy Records

4.1 Selecting a Contractor

When selecting a contractor, government agencies should take into account security considerations, methods of destruction available and whether a company is willing to provide documentation as supporting evidence that destruction has occurred. It should be noted that all contracts relating to the handling of public records must contain a clause, as described in s. 17(2) of the *Information Privacy Act 2000*, through which information privacy is transferred from the agency to the contractor. If this clause is not included in the contract, and if the contractor breaches the Information Privacy Act by mishandling personal information, the agency as well as the contractor will be held responsible under the Information Privacy Act. Further information concerning destruction of high security documents can be obtained from Privacy Victoria.

4.2 Responsibilities

Government agencies may engage contractors to destroy records. It remains the responsibility however, of the government agency to ensure that destruction is performed appropriately.

4.3 Transport of Records

Records may be transported by contractors or by the agency themselves. Where possible a closed truck should be used. If not practicable, the records should be secured by a cover. If the records are of a sensitive nature, they should only be transported in a closed and lockable vehicle (with locks engaged).

4.4 Documentation

Government agencies should insist on a certificate of destruction as part of their agreement with the contractor. If the records supposedly destroyed are subsequently found, the certificate is the evidence that the contractor is at fault, not the agency. It is recommended that the certificate also specify the method of destruction used.

5 References

Attorney-General's Department 2009, *Protective Security Manual (PSM)*, Australian Government, Canberra, viewed 19 March 2010, <[http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual\(P SM2005\)](http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(P SM2005))>.

National Archives of Australia 2010, *Destroying Records*, National Archives of Australia, viewed 10 March 2010 <<http://www.naa.gov.au/records-management/keep-destroy-transfer/sentencing/destroying.aspx>>.

RMIT 2007, *Guidelines for the Destruction of Records*, Royal Melbourne Institute of Technology, viewed 10 March 2010 <<http://mams.rmit.edu.au/rq5erohozhgx.pdf>>.

State Records of NSW 2005, *Destruction of Records: A Practical Guide*, State Records of NSW, viewed 10 March 2010 <<http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/guidelines/guideline-3>>.

Queensland University of Technology 2010, *Records Destruction Guidelines*, Queensland University of Technology, viewed 10 March 2010 <http://www.governance.qut.edu.au/rms/retention_disposal/Destruction_Guidelines.jsp>.

University of Technology Sydney 2009, *Undertaking Records Destruction*, University of Technology, viewed 10 March 2010 <<http://www.records.uts.edu.au/procedures/destroying/index.html>>.

Moreq2 (Model Requirements for the Specification of Electronic Records) 2008, *MoReq Specification*, European Commission, viewed 6 April 2010 <<http://www.moreq2.eu/moreq2>>.

Legislation

Public Records Act 1973 (Vic)

Information Privacy Act 2000 (Vic)

Crimes (Document Destruction) Act 2006 (Vic)

Evidence Act 2008 (Vic)

All current Victorian legislation is available at <http://www.legislation.vic.gov.au>

Other Resources

For more information about record destruction, please contact

Appraisal & Documentation Team
Public Record Office Victoria
Ph: (03) 9348 5600
Fax: (03) 9348 5656
Email: agency.queries@prov.vic.gov.au
Web: www.prov.vic.gov.au

Appendix 1: Checklist for Records Destruction

Before Destruction

Question	Yes	No	Unsure	Comments
Are the records authorised for destruction under a relevant and current RDA, SIDA or NAP?				
Are the records no longer in use?				
Has it been ascertained that the records are not the subject of current or pending litigation, FOI requests or a disposal freeze?				
Has internal authorisation been obtained and documented?				
Do the records have specific security requirements? (If yes, has the appropriate method of destruction been selected?)				

After Destruction

Question	Yes	No	Unsure	Comments
Has a certificate of destruction been produced?				
Was an appropriate method of destruction used?				
Has the destruction register been updated?				