Guideline No.3

Destruction of Records

A Practical Guide

1996 / Revised July 2000 / Revised December 2003 / Revised 2005

Summary

These guidelines have been prepared for personnel in New South Wales public offices who are responsible for arranging the destruction of records. It is designed to provide sound practical advice on physical destruction of records regardless of format.

In these guidelines

---

1 Introduction

Legal requirements

The disposal of state records is subject to the terms of the *State Records Act 1998* (NSW). Under the Act there are a number of ways to legally dispose of State records:

- with the permission of State Records through general retention and disposal authorities (GDAs), covering common classes of records created by public offices, or functional retention and disposal authorities (FRDAs), covering the records that document the role of a particular public office
- under provisions of certain legislation that authorise the destruction of certain records
- in accordance with 'normal administrative practice' (NAP). NAP covers the destruction of ephemeral records of a facilitative nature. For further information on NAP see Guideline 8: Normal Administrative Practice
- by an order of a court or tribunal
- in accordance with a resolution of a House of Parliament, in relation to a State record for which the House is the responsible public office.

Penalties

The State Records Act (Part 3, s.21) imposes a penalty for the illegal disposal of State Records. Agencies must be able to account for their records. If you destroy a record, you must be able to explain how and why this was undertaken. If you are not sure whether you have approval for destruction, contact State Records.

Summary of process

When considering the destruction of records, it is necessary to follow a number of principles. In summary, it is important to ensure that:

- the records have been authorised for destruction in accordance with the requirements of the *State Records Act, 1998*
- the records are no longer required under any other legislation (you have fulfilled all statutory and regulatory requirements), and that they are of no further administrative or business use to the organisation
- there is documentation identifying which records have been destroyed, when they were destroyed, how they were destroyed and under what disposal authority; and
- the records have been destroyed in a confidential and appropriate manner.

---

2 Principles of Destruction

Records destruction should be:

- authorised
- appropriate
- secure/confidential

- timely, and
- documented.

These principles are dealt with in more detail below.

Authorised

There are at least two levels of authorisation required for the destruction of records:

- formal disposal authorisation by State Records, usually in the form of a GDA or a FRDA, and
- internal authorisation (signing off) through an organisation's internal approval process.

Authorised by State Records

GDAs and FRDAs are the legal instruments which provide the formal disposal authorisation upon which a public office can act. They set a minimum period for retention. A record which is authorised for destruction in an approved and current disposal authority may be destroyed at the end of the appropriate retention period, if it is no longer required by the public office. For advice on applying disposal authorities to records, see guidelines on Implementing a disposal authority.

Authorised by Organisation

While disposal authorities set a minimum period for retention, it is also important to ensure that the organisation has no further business or legal needs for the records. This can be done by ensuring that there are appropriate internal authorisation or approval processes in place, for example, by providing appropriate staff with lists of records due for destruction.

A public office must not dispose of any records required for current or pending legal action or where the records may be required as evidence in a court case. A public office should not destroy records that are the subject of a current or pending Freedom of Information (FOI) request or any other statutory access request.

Once all requirements for retaining records have been met, an appropriate officer should give the final internal approval for the destruction of records. Each organisation should ensure that an officer is nominated and made responsible for this process.

Appropriate

Appropriate methods for destruction are:

- irreversible, and
- environmentally friendly.

These are dealt with in more detail below. Suitable methods of destruction for different media are covered in Methods of destruction.

Irreversible

Destruction of records should be irreversible. This means that there is no reasonable risk of the information being recovered again. Failure to ensure the total destruction of records may lead to the unauthorised release of sensitive information.

A number of cases have been reported in the media where records have been found "unearthed" in local garbage tips after they had been buried, or left in cabinets that had been sold. Records have also been found on the hard drives of computers that have been sold. Such occurrences are very bad publicity for your organisation and the New South Wales Government as a whole.

Environmentally friendly

Records should be destroyed in an environmentally friendly manner. Both paper and microforms should be recycled where possible.

Secure / Confidential

Records should always be disposed of with the same level of security that was maintained during the life of the records. Wherever possible, destruction of records should be supervised by an officer of the organisation or by another authorised agent if destruction has been contracted out.

Extra care should be given to records containing sensitive information (see also Sensitive information, below). Section 12 of the *Privacy and Personal Information Act 1998* states that a public sector agency must dispose of sensitive personal information securely to ensure the information is safeguarded against loss, unauthorised access, use or disclosure.

Lockable ‘wheelie’ bins may be used for particularly sensitive records. Sensitive records that are not binned should be transported in totally enclosed and lockable vehicles (to prevent records falling off the back of trucks!) and destroyed in the presence of an officer of your organisation. Sensitive records may also be shredded ‘in-house’ before being sent for pulping. Any in-house shredding should still be approved through the normal internal and external approval processes.

Timely

While records should not be destroyed while there is still a need for them, it is also important not to keep records longer than is necessary, to minimise storage costs and retrieval efficiency. If a decision is made to retain records longer than the minimum retention period a record of the reasons for the decision should be documented to assist disposal at a later date.

Records are usually destroyed when they have reached the end of a specified retention period. However, prior to their destruction, you must ensure that the records are no longer required. Therefore timely destruction must be balanced by internal authorisation.

Documented

The destruction of all records must be documented, so that your organisation is able to ascertain whether a record has been destroyed. Proof of destruction may be required in legal proceedings or in response to FOI requests.

Recordkeeping systems and any other documentation should note which Disposal Authority and disposal class authorise the destruction of the records. The specific

DA number and the disposal class number, for example GDA 7 class 1.1.2, should be documented along with the date of destruction.

You may also wish to keep a destruction register that would link individual records to be destroyed to consignments sent for destruction. This register, together with a certificate of destruction, will serve as proof that records have actually been destroyed.

The certificate of destruction should be placed on a file together with any other destruction documentation, for example, records of internal approval. A record of the method of destruction should also be placed on the file if this is not already noted on the certificate of destruction.

---

3 Methods of Destruction

There are a number of different methods of destruction appropriate for the different media on which the records are stored. These methods have been outlined below.

Paper records

Shredding

The security provided by the shredding of records depends on how fine the paper is shredded. Cross shredding may be needed for particularly sensitive documents. Shredded paper may be pulped and recycled, or may be used for insulation or other purposes.

Pulping

Pulped paper is reduced to its constituent fibres. If carried out correctly, it is a very secure method of destruction. Pulped paper is usually recycled.

Burning

Records should only be burnt if there is no environmentally friendly method of destruction available. Records should be burned in accordance with any environmental guidelines and local burning restrictions. Densely packed paper does not burn well, so burning should be undertaken in an industrial facility (not in a ‘backyard’ incinerator).

Important: Burying is not an appropriate method of destruction. The records are not destroyed immediately and may take months or even years to break down. Records that are buried may also be uncovered within hours or days of being buried.

Electronic / magnetic media

Magnetic Media

Records stored on magnetic media can be "bulk erased" by subjecting them to a strong magnetic field. For secure destruction magnetic media can be reformatted. Backup copies of the records also need to be destroyed. The media can then be reused. Note: just deleting does not remove data from magnetic media and is therefore not sufficient for the destruction of records.

Optical Media

Records held on optical media can be destroyed by cutting, crushing, or other physical means of destruction. Rewritable optical disks should also be reformatted before being disposed of or re-used.

Hard drives

Hard drives of personal computers and servers should be reformatted before computers are disposed of.

Important: Do not just delete files from electronic media such as floppy disks, rewritable optical disks and hard disks, as the information can be recovered.

Non-Electronic and non-paper media

Videos, cinematographic film and microforms (microfilm/ fiche/ aperture cards/ x-rays) can be destroyed by shredding, cutting, crushing or chemical recycling.

---

4 Using a Contractor

Responsibilities

Contractors can be engaged to destroy records. However, it is the responsibility of the public office to ensure that destruction occurs in accordance with the approved methods of destruction. Make sure you know what method of destruction your contractor is using.

Transport of records

The contractor can collect records from your office for destruction, or you can deliver the records to them. A closed truck should be used whenever possible. However, if there is no alternative and the contractor can only provide an open truck, ensure that the load is secured by a cover. Sensitive and confidential records should only be conveyed in a closed and lockable vehicle.

Documentation

Always insist on a certificate of destruction. If records that were supposed to be destroyed are subsequently found, the certificate is evidence that the contractor was at fault, not your organisation. You may also want to request that the certificate of destruction includes the method used.

Contract 6083 - Secure Destruction Services

Contract 6083 is a period contract for the provision of Secure Destruction Services and is available for the use of Government departments, agencies and authorised users of State Contract Control Board Contracts. The contract is managed by State Procurement and further details of the contract are available at www.stateprocurement.ogp.commerce.nsw.gov.au

---

5 Sensitive Information

There are different types of sensitive information to be aware of. Particular care must be taken in handling and destroying sensitive information.

Personal information

Public offices collect a great deal of information about individuals, and much of this information is quite sensitive, for example criminal, health or welfare records. Even records relating to the licensing of drivers, professions, trades, and commercial activities may contain personal information that could be sensitive. All personal information must be managed in accordance with the requirements of the *Privacy and Personal Information Act 1998.*

Personnel files are a prime example of records containing personal information that have strict access/security restrictions while the records are active. This level of security should be maintained throughout the entire life of these records including during the destruction process.

Financial or commercially sensitive information

Records may contain information of a commercially sensitive nature. Examples include files containing information on an organisation's financial position, tender bids, and any information that may give an unfair financial advantage to another.

Information given in confidence

Records may contain information that is given on condition that the information is not released. Examples include personal information and financial information, information given by government agencies (foreign governments, interstate/federal bodies) and information from any source where the provider specifies that it is given in confidence.

Information relating to an investigation

Records relating to an investigation, usually into malpractice or criminal activity, may contain sensitive information. With such records, it is important to ensure that sensitive information is not released through inadequate or inappropriate destruction techniques.

Information posing a security risk

Records may contain information dealing with high security risk activities and premises. Examples of such records are plans of buildings for correctional institutions or banks, procedures for the delivery of large amounts of money, and security arrangements for movements of heads of State.

Appendix A: Checklist for records destruction

❑	The records are authorised for destruction under a relevant and current disposal authority

❑	The organisation no longer requires the records
❑	The records are not the subject of a current or pending court case or FOI request
❑	Internal authorisation has been obtained
❑ ❑	The records have no special security requirements OR The records have high security level and locked bins and/or in-house shredding are required for security destruction
❑	Appropriate service provider contacted
❑	A covered van/truck specified for records removal
❑	Service provider asked to supply certificate of destruction
❑	Specified that records are to be destroyed on day of collection
❑	Certificate received by organisation
❑	Records destroyed and details of destruction documented in the organisation's records system.

State Records Authority of New South Wales
Sydney, Australia

Revised Edition December 2005

ISBN 0-7313-5355-2