

How do I destroy records?

SUMMARY

How do I destroy records? is the sixth part of an FAQ series on disposal. It outlines:

- what destruction is
- destruction principles and methods.

WHAT IS DESTRUCTION?

Destruction is the process of eliminating or deleting records, beyond any possible reconstruction.¹ There are many methods for destroying records; the method chosen depends on the media.

Media

Media is a generic term for hardware, often portable in nature, which is used to store data.²

Media sanitisation

Media sanitisation is the process of **erasing** or **overwriting** data stored on media so it cannot be retrieved or reconstructed.³

Some media cannot be sanitised, and sometimes, sanitisation fails. In these cases, the media is destroyed.

Media destruction

Media destruction is the process of physically damaging media with the intent of making data stored on it inaccessible. Only the actual material in which data is stored needs to be destroyed.⁴ Common methods include **disintegrator**, **hammer mill**, **shredding** and **pulping**.

Some methods, like **degaussers**, can sanitise media and destroy it. This depends on the media and the magnetic force applied.

Inappropriate destruction methods

Inappropriate destruction methods including burning, burying, deletion and dumping.

Burning is a last resort if no other destruction method is available. Burning causes unnecessary environmental pollution. Densely packed paper does not burn well, so burning should only take place in an industrial facility.

Burying. Records may be uncovered after burial. It can take months or years for paper records to break down.

Deletion. Deleting records from media such as a hard drive does not permanently erase them. Only the link to the data (such as the file name and directory path) is deleted. Data may be restored for some time after deletion.

Dumping. This does not destroy records, and records may be found after dumping.

WHAT ARE THE GENERAL PRINCIPLES FOR DESTROYING RECORDS?

Our *Information and Records Management Standard* states:

'Records should be destroyed in a way that is authorised, timely, documented, secure, safe, environmentally friendly and appropriate for the media.'

These principles are explained more below.

Authorised

Use authorised Disposal Schedules and one-off Destruction Authorities. These are legal instruments authorised by the State Archivist that allow you to destroy records.

Follow your organisational policies and procedures and ensure delegated officers approve destruction.

Timely

Destroy time-expired records regularly. This will minimise your storage costs and improve efficiency. It will also meet privacy legislation and reduce the risk of unauthorised disclosure.

Documented

Document your organisational records disposal programme. This helps prove your disposal and destruction is controlled and legally defensible.

Maintain a *Register of Records Destroyed* as evidence of your lawful records destruction.

If you outsource destruction, get a certificate of destruction that includes the method of destruction. If supposedly destroyed records are later found, the certificate is proof that the contractor was at fault.

Secure

Ensure your records destruction is secure, whether completed in-house or outsourced. If moving records off-site, transport them in closed vehicles and ensure paper records are in locked bins. This will help prevent loss, theft and unauthorised disclosure.

Supervise destruction on at least the first time that you use a new commercial destruction provider.

Take extra care with high-value, high-risk records. This includes sensitive and security classified records, and those that contain personal information.

Safe

Follow work health and safety requirements and limit exposure to dangerous substances. Some media contains arsenic, lead, mercury etc. These may be poisonous, carcinogenic or toxic in particulate or dust form.

Environmentally friendly

Use the most appropriate destruction method with the least adverse environmental impact and recycle where possible.

Appropriate

Use the most appropriate destruction method for the media.

HOW DO I CHOOSE THE RIGHT DESTRUCTION METHOD FOR THE MEDIA?

Physical media

The Australian Signals Directorate produces the *Information Security Manual* (the *ISM*). The *ISM* is an authoritative source of information about sanitisation and destruction methods. It is updated regularly.

The 'Guidelines for information technology equipment' and 'Guidelines for media' sections⁵ cover most types of physical media.

Contact us for advice if you wish to destroy media that does not fall into one of these categories.

Cinematographic film and x-rays

Shred, cut, crush or use chemical recycling.

ICT and media equipment

Includes:

- hybrid hard drives
- network devices
- printers and multi-function devices
- solid-state media
- volatile media, etc.

Magnetic media

Includes:

- audio reel-to-reel and cassette tapes
- computer tapes
- floppy disks
- hard disk drives (HDD)
- video home system (VHS) tapes etc.

Media that cannot be sanitised

Some media cannot be sanitised and must be destroyed. This includes:

- microfiche and microfilm
- optical disks
- programmable read-only memory
- read-only memory.

Media that cannot be sanitised successfully

Some media cannot be sanitised successfully. For example, sanitisation may fail because the media is faulty or damaged. In this case the media is destroyed. Use a method appropriate to the media.

Microform

Includes:

- aperture cards
- microfiche
- microfilm etc.

Optical media

Includes:

- Blu-Ray discs (BD)
- compact discs (CD)
- digital video discs (DVD) etc.

Systems

Back-ups

Destroy according to the *Disposal Schedule for Short Term Value Records (DA2158)*. Use a method appropriate to the media.

Business Systems and Electronic and Records Management Systems (EDRMS)

Destroy records using the functions of the system.

If you plan to decommission the system, seek advice from our Office.

Paper

Shred and pulp paper. Once pulped, recycle.

HOW DO I DESTROY THE 'AUTHORITATIVE' RECORD?

Traditional records management advice about destruction uses phrases like 'irreversibly destroyed'. Completely destroying paper records by shredding, pulping and recycling is simple and verifiable. Destroying digital records is more complex.

Digital records are easy to copy and share. Copies of records stored in approved records management systems may be also stored:

- on mobile devices
- as email attachments
- on personal, shared or hard drives
- in collaborative workspaces like Teams
- in other business systems
- in cloud based systems
- on Intranets and websites
- in back-up systems
- by other organisations.

Finding and irreversibly destroying all copies of records may be:

- time-consuming
- resource intensive
- impractical.

We recommend you destroy the 'authoritative' record. Mostly, this will be in your records management system.

Focus on your high-value, high-risk records, and consider their classification and sensitivity. Document your approach in your policies. For example, you might want to treat copies in other systems as duplicates or working drafts.

INFORMATION SECURITY

Tasmania's *Protective Security Policy Framework* (the *TAS-PSPF*) sets out nationally consistent standards. It aims to protect Tasmanian Government information, people and assets from compromise and harm.

The *TAS-PSPF* applies to some, but not all, of the organisations subject to the *Archives Act 1983* (Tas).

If your organisation is subject to the *TAS-PSPF*, use it alongside this advice. *INFOSEC-2: Protecting Official Information (INFOSEC-2)* is the most relevant part of the *TAS-PSPF*. This contains additional requirements for sensitive and security-classified information.⁶

ACKNOWLEDGEMENTS

This FAQ is based on and replaces:

- *State Records Guideline No 21: Approved Destruction Methods for State Records*.

We also acknowledge the following publications:

- Archives New Zealand (2023) [Methods of Destruction](#), Version 2 July 2023, ANZ website, accessed 12 May 2026.
- National Archives of Australia (n.d.) [Compliant Destruction of Australian Government Information](#), NAA website, accessed 12 May 2026.
- Public Record Office of Victoria (2024) [Destruction: Information about Destroying Records](#), 4 March 2024, PROV website, accessed 12 May 2026.
- State Records NSW (2025) [Destruction of Records](#), 30 January 2025, SRNSW website, accessed 12 May 2026.
- State Records Office of Western Australia (2026) [Records Management Guideline: Records Retention, Disposal and Destruction](#), March 2026, SROWA, accessed 12 May 2026.

REFERENCES

¹ Office of the State Archivist *Glossary*.

² *ISM* 'Cyber security terminology'.

³ *ISM* 'Cyber security terminology'.

⁴ *ISM* 'Cyber security terminology'.

⁵ *ISM* 'Guidelines for information technology equipment' and 'Guidelines for media'.

⁶ *TAS-PSPF: INFOSEC-2*: 'Required action: securely dispose of sensitive and security-classified information' and 'Annexure 7 – minimum handling protections for disposal of sensitive and security-classified information, ICT and media equipment'.

MORE INFORMATION

- Australian Government, Australian Signals Directorate (2026) [Information Security Manual \(ISM\)](#), March 2026, ASD, accessed 12 May 2026.
- Office of the State Archivist (n.d.) [Glossary](#), OSA website, accessed 12 May 2026.
- Office of the State Archivist (2026) [Information and Records Management Standard](#), Version 1.2, OSA, accessed 3 June 2026.
- Office of the State Archivist (n.d.) [Register of Records Destroyed Template](#), OSA, accessed 12 May 2026.
- Office of the State Archivist (n.d.) [Retention and Disposal Schedules](#), OSA website, accessed 12 May 2026.
- Tasmanian Government, Department of Premier and Cabinet, Resilience and Recovery Tasmania (2025) [Tasmania's Protective Security Policy Framework: Information Security INFOSEC-2: Protecting Official Information \(TAS-PSPF INFOSEC-2\)](#), Version 2.1 December 2025, DPAC, accessed 12 May 2026.

Documents in this series are:

- *What is disposal?*
- *What is a Disposal Schedule?*
- *How do I use a Disposal Schedule?*
- *How do I get a Disposal Schedule?*
- *Disposal Schedule conventions*
- *How do I destroy records?*

CONTACT US

Office of the State Archivist | <https://osa.tas.gov.au> | enquiries@osa.tas.gov.au | 03 6165 5581

How do I destroy records? is part of the *Tasmanian Government Information Management Framework*. It supports the *Information and Records Management Standard*. This is a living document and we will make minor changes as needed. If you notice anything that needs updating, please let us know.



License URL: <https://creativecommons.org/licenses/by/4.0/>
Please give attribution to: © State of Tasmania, 2026.

Document Development History

Version	Date	Comments
1	3 June 2026	Initial release