

# Methods of destruction

---

## 1 Introduction

Under Section 18(i) of the *Public Records Act 2005* (the Act), a public record or a protected record cannot be destroyed without the authorisation of the Chief Archivist. When a public office or a local authority destroys information and records, it must ensure that it follows the appropriate guidelines and procedures.

## 2 Reasons for destruction

Information and records should be destroyed using the correct method and at the appropriate time. This is important because it:

- saves time and storage costs
- shifts focus to higher priority information and records
- prevents unauthorised access to information and records
- may be a legislative requirement (such as to ensure privacy conditions are met).

## 3 Which information and records have to be destroyed

Only destroy information and records that the Chief Archivist has authorised for destruction.

For public offices, there are three types of disposal authorities:

- organisation specific disposal authorities set for a limited period
- one-off disposal authorities created for specific records
- general disposal authorities, issued by Archives New Zealand for records commonly kept by a public office.

For local authorities, the Association of Local Government Information Management (ALGIM) has an example retention and disposal schedule. The schedule is part of its Information Management Toolkit. This example shows information management staff at local authorities how to decide whether to retain or dispose of their non-current (or inactive) information and records. In addition, the List of Protected Records identifies categories of information and records that the Chief Archivist classifies as “worthy of protection”. These records can only be destroyed with the approval of the Chief Archivist.

Check with your staff whether any information and records considered for destruction are needed for ongoing business needs. Also, check whether these records need to be kept for compliance reasons. You will need to keep information and records in your organisation if they are:

- part of a request under the Official Information Act 1982
- part of a request under the Local Government Official Information and Meetings Act 1987
- part of an appeal to the Ombudsman.

Only the Chief Archivist can authorise the transfer to a third party of any information and records approved for destruction.

## 4 Ways to destroy information and records

Destruction in any form should be irreversible, secure and documented. Take extra care when destroying sensitive information and records. Ensure that they are not accessible by mistake or without authorisation. In addition, burying or dumping is not a secure disposal method. Someone may find and retrieve it.

Use the most appropriate destruction method that has the least adverse environmental impact. Archives New Zealand recommends the destruction methods noted in the table below.

Type	Recommended destruction method
<b>Paper</b>	<p>Shred documents that do not hold highly sensitive information.</p> <p>Burn or pulp documents that hold highly sensitive information.</p>
<b>Digital</b>	<p>Clear or overwrite non-secure digital information to ensure no one can retrieve or read the information or record (including the metadata). Deletion is not destruction. Deletion only removes the link within the system to the information or record, rather than the information or record itself.</p> <p>Destroy secure digital information to ensure no one can use the information or record (including the metadata), or the media on which it is held.</p>
<b>Other media</b>	<p>Cut, crush, shred or use chemical recycling appropriate to the type of media being destroyed. Examples of magnetic and optical audio-visual media are film, video, audiotape and microforms.</p>