

---

# Information Management policy

## Overview

Information is a corporate asset, vital both for ongoing operations and also in providing evidence of business decisions, activities and transactions. As an asset, our information is needed to:

- Facilitate information accessibility and enhance business by supporting program delivery, management and administration;
- Deliver customer services in an efficient, fair and equitable manner;
- provide evidence of actions and decisions, as well as precedents for future decision making; and
- Protect the rights and interests of the Australian Commonwealth Government and its citizens.

The department's policy is that all information is managed in a manner consistent with the National Archives of Australia (NAA) guidelines, associated legislation and endorsed standards. The policy has been designed to ensure staff are able to meet their obligations when working with information.

The benefits of compliance with this policy will be trusted information that is well-described, stored in known locations, and accessible to staff and clients when needed.

## What is the purpose of this policy?

The Information Management policy will implement fit-for-purpose information management practices to ensure the creation, maintenance and protection of information. All information management practices in the department are to be in accordance with this policy and its supporting documentation.

Information Management must ensure that the department:

- Has the information it needs to support and enhance ongoing business and customer service, meet accountability requirements and community expectations;
- Manages information efficiently, so that it can be easily accessed and used for as long as required;
- Stores information as cost-effectively as possible and - when no longer required –disposes of it in a timely and efficient manner;
- Complies with all requirements concerning information management practices, including the Australian Commonwealth Government’s objectives for information management; and
- Identifies and protects information of longer term value for analysis, historical and other research.

## What is the scope of this policy?

This policy applies to all users of department information assets including department employees, suppliers, business partners, and contractors, irrespective of their geographic location.

It applies to all hard-copy and electronic information formats including documents, email, voice messages, memoranda, minutes, audio-visual materials and business system data.

It applies to the creation, collection, sharing, publication, and disposal of information.

This policy also covers all business applications used to create, manage and store information including the official information management systems, email, websites, social media applications, databases and business information systems. This policy covers information created and managed in-house and off-site.

## What are my responsibilities?

Position	Responsibility
Chief Information Officer (CIO)	<ul style="list-style-type: none"> <li>• Has ownership of the Information Management Policy, and oversees the implementation and management of this policy within the department.</li> <li>• Ensure that Information Management is adequately resourced.</li> <li>• Represents information management interests to the Deputy Secretary and Secretary.</li> </ul>
Chief Information Governance Officer (CIGO)	<ul style="list-style-type: none"> <li>• Ensure that the department complies with the requirements of all Commonwealth legislation relating to information management.</li> <li>• Ensure support of, and adherence to, this policy by promoting a culture of compliant information management within the department.</li> </ul>
General Managers	<ul style="list-style-type: none"> <li>• Ensure that information is created and managed within their business unit in a way which complies with the Information Management Policy.</li> <li>• Provide feedback on the success of management processes to help ensure information remains accurate, fit for purpose, complete, available and accessible, well presented, meaningful, and relevant.</li> <li>• Ensure that staff are trained in how to create and manage information.</li> <li>• Consult with the Information Managers when introducing new activities and systems.</li> <li>• Ensure that contract with service providers contain information management clauses in accordance with this Information Management Policy</li> </ul>

Position	Responsibility
Information Managers	<ul style="list-style-type: none"> <li>• Comply with Information Management Policy, guidelines, and endorsed standards in relation to all aspects of information management.</li> <li>• Monitor compliance with the Information Management Policy, and make recommendations for improvement or modification of practices.</li> <li>• Advise on information management systems.</li> <li>• Establish and maintain a standard metadata schema and business rules regarding how metadata is to be managed, in liaison with the <b>DatMAT</b> team.</li> <li>• Advise on risks associated with non-compliance.</li> </ul>
Agency Security Advisors	<ul style="list-style-type: none"> <li>• Provide advice on security policy and guidelines associated with the management of information.</li> </ul>
Information Officers	<ul style="list-style-type: none"> <li>• Responsible for the conduct of records management operations.</li> <li>• Ensure that information management policies and projects take into account the special nature of records.</li> <li>• Establish and maintain a standard recordkeeping metadata schema and business rules regarding how metadata is to be managed.</li> </ul>
ICT Operations and Security	<ul style="list-style-type: none"> <li>• Support and maintains ICT infrastructure necessary for the delivery of department business information systems.</li> <li>• Implement information security measures (including accessibility), in accordance with department Information Security Management Policy.</li> <li>• Perform routine and comprehensive system backups of data.</li> <li>• Ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy</li> </ul>
Corporate Communications	<ul style="list-style-type: none"> <li>• Creation and management of organisational templates, including for email.</li> </ul>

Position	Responsibility
Staff	<ul style="list-style-type: none"> <li>Comply with Information Management Policy, guidelines, and endorsed standards.</li> </ul>
Contractors, service providers, suppliers, and business partners.	<ul style="list-style-type: none"> <li>Manage information that they create on behalf of the department according to the terms of their contract.</li> </ul>

## What is Information?

For the purposes of this policy, 'Information' is:

- knowledge about some fact, subject or event;
- that is in digital or paper form; and
- that is used by the department while undertaking its business.

Information can be characterised by how *structured* or *unstructured* it is. Structured information is typically referred to as '**data**' is stored in a specific data model, and is managed by a database e.g. the **TechnologyOne** finance system, and the **Lighthouse** analytics and reporting system.

The department has a data governance framework plus accompanying policies and practices that must be followed in conjunction with this information management policy.

- View the **Data Governance Framework** and **Data policies** for more details.

Examples of information that can be considered *unstructured* include:

- Documents e.g. Microsoft Word, Excel, PowerPoint, Visio, etc.
- Email and other correspondence.
- Audio-visual files e.g. videos, animations, pictures, sound recordings, etc.
- Web pages and other online content - including social media posts - published for, or on behalf of, the department.

Information created, sent and received as Australian Government business is a **Record**. This information provides evidence of what our agency has done and why.

All records must be kept and managed in accordance with National Archives Australia policies and related legislation.

- View [Making and keeping records](#) for more information.

## Information that must be retained or can be destroyed

All information created and managed by the department will be either:

- Transferred to the NAA for permanent retention because it has significant value and is part of our national story; or
- Destroyed under an NAA issued instrument called a **Records Authority**. Destruction can occur only after permission is granted by the owners of the information.

Some records can be destroyed in the normal course of business. These are records of short-term value and are destroyed as a Normal Administrative Practice (NAP). These include rough working notes, drafts not needed for future use, and duplication of information held for reference.

- View [Legally destroying information and records](#).

## Where should I keep my information?

When you are creating or working with information in documents or files (e.g. refer to *unstructured information* above), this digital information should be kept in DocHub or in Content Manager.

Whenever possible, documents and files should *begin* and *end* their life in DocHub or in Content Manager i.e. be managed via automatic version control from the first draft onwards as they evolve to a final version.

## Protected network

For staff on the Protected network, digital information should be kept in DocHub – the department’s SharePoint-based document collaboration system.

Information should only be printed and stored on paper if it is an approved exception, managed by the Information Management section.

A small number of business areas still manage their information digitally in the Content Manager system, and may continue to do so unless otherwise advised.

For more information see:

- [DocHub](#)
- [Content Manager](#).
- [Titling guidelines for files and documents](#)

## Approved exceptions

Information that is security classified Secret or Top Secret, which must meet explicit legislative requirements, or cannot be digitised (e.g. samples of materials) must be managed physically. There are very limited circumstances where paper records should be created.

- [View Scanning](#).

## Unclassified network

Staff on the Unclassified network should continue to work in their current recordkeeping systems e.g. Content Manager, unless otherwise advised.

## What format should I use when saving information?

It is important that information assets remain accessible and usable over time. Files and documents created now may need to be retained and referred to for many years to come, and in some cases will be kept indefinitely.

Information that is identified as being of permanent (or continuing) value will be sent to National Archives Australia. Such information is of national significance or public interest and will continue to have value to the Australian Government and the community for generations to come.

In general, the default file format used by common business applications provided to you in the department's standard desktop environment (such as Microsoft Word, Excel, PowerPoint, Outlook, etc.) are suitable for long-term use.

However, specialised business applications and technical software may use proprietary file formats that are unsuitable or unsafe for long-term retention.

Wherever possible, information should be saved in file formats that use open standards and that have fully documented technical specifications.

- [View Acceptable file formats](#)

The Information Management section will ensure that information stored in acceptable file formats remains accessible and usable throughout its lifespan and until its disposal.

If you are unsure about a business application or software tool you are using and need more information, [Lodge a request with Information Management](#) or phone

s 22

## What about information security?

All users of department information assets including department employees, suppliers, business partners, and contractors have a responsibility to protect our information and use it appropriately.

The Information Security Policy defines how the department maintains an acceptable standard of information security, and defines user responsibilities in detail.

- [View the Information Security Policy.](#)

## Information security classification

Security classification must be applied to information when it is created or captured.



Information security classification is a requirement under the **Protective Security Policy Framework**. Classifications are used to indicate the value of information and the level of protection that information needs.

- View **Security classification for files and documents**.

## How do I manage information privacy?

The **Australian Privacy Principles** and the **Privacy Act 1988** regulate how the department collects, uses, discloses and stores personal information.

- View the **Privacy** information provided by **legal services** for more information.
- View **Personal Information Breach – Notification Policy**

## What do I do if I need to transfer information?

### Internal transfers




The Information Management section must be advised if you transfer physical information to another staff member or between locations.

### External transfers

If the transfer of information is due to a Machinery of Government (MoG) change or staff transferring to other Australian Government departments, advise the Information Management section.

- View **Transferring and returning files** for more information.

## Where can I find more information?

- DocHub
- Content Manager
- Document and file storage policy
-  Handling an organisation's personal information - Data security breach notification policy (PDF 103KB) |  (DOCX 83KB)
- Making and keeping records
-  Open by default policy (PDF 103KB)

- Recordkeeping and eLearning modules from National Archives
- Scanning
- Records Disposal Authorities for the department
- Transferring and returning files

For a summary of Information Security Requirements, refer to **Appendix B** in the Data Governance Framework.

For a summary of legislation that applies to the department in regards to information management, refer to **Appendix C** in the Data Governance Framework.

For a summary Information Management standards and guidelines applicable to the department in regards to information management, refer to **Appendix D** in the Data Governance Framework.

---

## Contact us

- Lodge a request with Information Management

s 22

Home > Working here > About the department > Records and information management



# Records and information management

Records provide evidence, explain action, justify decisions and demonstrate processes followed. They are an essential part of a transparent and accountable public service.

This means the department's records need to be properly managed. To do this we have a records management system with rules around how we create, receive, maintain, use and dispose of our records and information.

These rules apply to all employees including SES, contractors and consultants.

## Benefits and obligations

By making and keeping records appropriately we are able to:

- access records when government actions are scrutinised under the *Freedom of Information (FOI) Act 1982*
- satisfy *Public Governance, Performance and Accountability Act 2013* requirements to properly document decisions to spend money
- comply with the *Archives Act 1983* when it comes to destroying records

- satisfy personal accountability requirements under the APS values and code of conduct.

Good records management also makes good business sense because it:

- builds corporate memory and embeds knowledge in the department
- improves productivity because easy access to shared information helps decision making, and means people don't have to reinvent the wheel
- protects the rights and entitlements of individuals and organisations.

We need to manage our records in a manner consistent with the:

- National Archives of Australia (NAA) guidelines
- associated legislation
- endorsed standards.

---

## Make and keep records

You must make and keep reliable and accurate records of your work-related activities. Records should be digital/electronic by default. Paper-based records are by exception only. Records can also include physical objects such as maps, test results or specimens.

You must:

- make records to support what you do
- manage records in the department's recordkeeping systems
- follow departmental policies and guidelines for the management of records.

You must not:

- destroy, delete or alter records
- remove corporate records from the department without permission

- lose any records that are in your care.

For more information see the [Creating records page](#) on the NAA website.

## Store records

The department has a 'digital by default' records management policy. This means you must store all records in a digital format (unless it is an [Approved exception](#)). There are very limited circumstances where paper records should be created.

Staff on the Protected network should keep their information in DocHub. You can find more information about using DocHub on the [Corporate systems page](#).

Staff not on the Protected network (e.g. NMI) should manage their digital information in [Content Manager](#). If Content Manager is not available (e.g. Questacon) then network shared drives may be used.

## Approved exception

You can only print and store information on paper if it is an approved exception. This includes information that:

- is security classified above PROTECTED
- cannot be digitised (e.g. samples of materials that must be managed physically).

In this instance please contact the Information Management section for assistance. See also the:

- [Departmental information storage policy \(PDF 84KB\)](#)
- [Digital continuity 2020 policy](#) on the NAA website
- [Preserving physical objects page](#) on the NAA website.

## Name files and documents

There are naming conventions you should follow when you create a title for your files or documents.

A file refers to a grouping of documents. A document refers to a piece of written, printed or electronic matter that provides information.


Titles should describe the functions and/or subjects documented in a record. A meaningful title supports its easy discovery throughout the life of a record.

## Titling checklist

When choosing a title for your files and documents, follow the guidance below:

- Choose a title that is specific and easy to understand.
- Spell out abbreviations and acronyms unless they are commonly known.
- Avoid vague terms like 'miscellaneous', 'general' or 'correspondence' unless it is appropriate.
- Avoid using jargon.
- Don't put version numbers in a title (this is captured automatically).
- Remove punctuation unless it is part of a registered brand or logo.
- Use an ampersand (&) in a title only if they are used in company names.
- Avoid full stops or underscores (\_). Use hyphens to separate text, with a space before and after the hyphen.
- When referring to numbers use a digit format except when the number forms part of a name.
- Write days and dates in full (except for birthdates).

For detailed guidance:

- see the  [Naming and metadata conventions: titling and tagging guide \(PDF 135KB\)](#)
- watch the [What's in a name](#) YouTube eLearning module developed by the NAA.

---

## Scan records

Paper files/records can be scanned by the Information Management section. The original record will be kept for an agreed period of time in consultation with the relevant business area. The Information Management section will then manage its lawful destruction.

A scanned copy must be quality assured as a true reproduction before its source document (original) can be legally destroyed. See the NAA website for [Digitisation specifications for paper records in agencies](#) .

Scanned information inherits the same security classification as the original document and must be managed accordingly.

Any document with an [Information security classification](#) above PROTECTED **must not** be scanned. Such information must be placed on an official paper file and registered in the department's official records management system, managed by the Information Management section.

## Scan a file

Information Management can provide advice on digitising paper files.

Email [s 22](#) for assistance.

## Scan a single document

Business units may scan individual documents received in paper format. If the document is part of a larger file that is not digitised, you should consult the Information Management section to ensure all the information is digitised together. This avoids us creating hybrid or partially digitised records.

Follow these steps to scan an individual paper document:

1. Scan using a multi-function device (MFD).
2. Verify that the electronic version is an exact copy of the original.

3. Store the electronic version in a records system (DocHub or Content Manager).
4. Destroy the original (shredder or secure destruction bin).

## Scan paper mail

You don't need to scan your paper mail documents. Paper mail is scanned by Mail services and sent to you electronically.

See the [Mail services page](#).

---

## Request a file

### Protected network

The department has a 'digital by default' records management policy. Paper files will not be created unless you have an exemption.

Check with Information Management before completing a file request form.

If Information Management approval is granted, use the [File request form \(PDF 87KB\)](#) to:

- create a new record
- create new file parts
- make changes to an existing file, including amending file titles
- amend the security classification.

Then lodge a request with Information management via [ServiceNow](#) and attach your completed form.



Pay attention to the security classification you apply to the file. You cannot assign a classification level higher than your own clearance level.

## NMI

You can request a file in NMI through Content Manager.

For detailed steps on how to do this, download  [How to request a new file through HPE Content Manager \(PDF 353KB\)](#).

---

## Transfer physical files

When transferring legacy physical files you must:

- inform Information Management of any transfer of records
- ensure there are no loose secure all papers, clips, tabs or plastic covers in the files.

## Transfer files internally

Return your files to Information Management or transfer them to another officer if you are:

- leaving the department
- moving sections
- taking extended leave.

When you transfer files to another officer you must:

- physically locate the files
- check the new recipient holds the appropriate security clearance (their clearance must be the same or higher than the file being transferred)

- gain acceptance from the new recipient for the transfer
- add their name, your signature and the date on the front cover
- advise Information Management so they can update the changes in the recordkeeping system.

## Transfer files externally

You must advise the Information Management Team if you plan to transfer records to another agency or department, or there is a Machinery of Government (MoG) change. This applies regardless of whether the records are in physical or electronic format.

---

## Return files

Physical legacy records that are no longer required for active use should be returned to the Information Management section.

Any files that are not registered in Content Manager will be returned to the relevant business area. Information Management staff will then assist with registering them as an official record.

To return a physical file to storage: [Lodge a request with Information Management](#) .

You will need to observe the correct security procedures when transporting files. See how to handle and share hard copies of PROTECTED, Secret and Top Secret files.

For instructions on delivering the files see [Delivering files to Industry House](#).

## Return bulk files

Before you return a large amount of files, you must advise the Information Management Team. In addition to the steps outlined above you must also prepare the files for transfer:

1. Place the files spine down into the box in numerical order from left to right.
2. Number the boxes in the format Box 1 of 20, Box 2 of 20 and so on.
3. Send an email to the addressee to let them know the delivery is on its way.
4. Leave a gap of about 5-10cm at the top of each box. Do not overfill boxes.
5. Check the weight of each box does not exceed 16kg.
6. List the contents of each box and place a paper copy on the inside of the box lid. Also email of copy of the lists to [s 22](#)
7. Secure and tape down the boxes so that files cannot be tampered with or unlawfully accessed.
8. Place a large label on the box (A4 if possible) with the address, receiver's name and the box number.

## Return NMI files

Use the [📄 NMI archival files indexed list template \(XLS 126KB\)](#) to label and list NMI records.

Contact the NMI Records Team via Information Management if you need to arrange archive boxes.

## Deliver files to Industry House

You must deliver all files to Industry house at the following address:

Department of Industry, Science, Energy and Resources  
Industry House  
Loading Dock in Akuna Street (drop-off point for courier driver)  
CANBERRA CITY ACT 2601

See Table 1 below for details on how to deliver files from each office.

**Table 1: File delivery procedures for each office location.**

Office location	File delivery procedure
Industry House	<p>Hand records directly to Information Management located at the mailroom on the ground floor.</p> <p>If you have more than five files or classified files, contact Information Management for alternative options.</p>
51 Allara Street & Questacon	Use your normal mail run to deliver files to Industry House.
ARENA (Nishi Building)	Use your own courier arrangements to deliver files to Industry House.
State and regional areas	Use your own delivery arrangements. Each business area must cover all associated costs, including archiving boxes and freight.

## Destroy records legally

Not all records can be destroyed. Under the *Archives Act 1983*, each record must be assessed before it can be destroyed. Please contact Information Management before destroying a paper file.

## Destroy low value information

There is a mechanism for agencies to dispose of low value information – such as rough working notes, drafts or duplicates – without formal authorisation. This is called normal administrative practice (NAP).

See [Normal administrative practice](#) on the NAA website for comprehensive guidance on the NAP process. It includes a checklist for you to confirm which information you can safely destroy.

## Destroy hard copy information and records after scanning

Once information has been scanned, the scanned image becomes the official record. Individual hard copy documents can be destroyed using NAP if they meet the requirements.

## Destroy high value information and records

Higher value records are covered by a records authority. These records are usually:

- for accountability purposes
- to support the ongoing administration of department business
- linked to community expectations about records providing rights and entitlements, or
- considered as having cultural or known historical value for the department.

Check with the Information Management section to determine if a records authority applies to your record. See also [Records authorities](#) on the NAA website.

---

## Disposal freezes

Holds may be placed on information and records as a result of disposal freezes. This means relevant information and records cannot be destroyed until the hold has been lifted. A hold supersedes a records authority or NAP – even if the information is due for destruction.

Records protected under a disposal freeze are often related to:

- prominent or controversial issues and events
- legal proceedings such as a Royal Commission or compensation cases
- FOI requests.

Under the *Crimes Act 1914* it's an offence to intentionally destroy documents required for a legal case. Legal Services and Information Management will work with business areas to agree on the appropriate way to manage this information.

The NAA website has [Current disposal freezes and retention notices](#) .

## Types of disposal freeze records

A disposal freeze will apply to any record due to be destroyed, including drafts and working papers. It will also apply to the following:

- Physical records such as paper, microfilm, magnetic tapes, recordings and photographs.
- Digital records from email, office applications, document management systems, shared spaces and drives, thumb drives, laptops and other official portable devices.
- Digital data from databases and business systems (e.g. finance, HR, CRM or workflow and case management systems). This includes the necessary metadata needed to search and display information.
- Records not captured in formal recordkeeping systems, including personal notebooks and unregistered files or folders. You must notify the Information Management Team if these records are not registered.





## How long to keep disposal freeze records

Records covered by a disposal freeze must be protected and made available until:

- the proceedings (including appeals) are completed

- confirmation that the records are not required.

## Further information

-  [Information Management Governance Framework](#)
-  [Open by default policy](#)
-  [Handling an organisation's personal information - data security breach notification policy](#)
- For information about using DocHub go to the [Corporate systems page](#)
- For information about using Content Manager go to the [Content Manager page](#)
- [Secure official information page](#)
- [Lodge a request with Information Management via ServiceNow](#) 

s 22

s 22

