Australian Government
Department of Education, Skills and Employment

Information Management Policy

ISBN

xxx-x-xxx-xxxxx-x [PRINT]
xxx-x-xxx-xxxxx-x [PDF]
xxx-x-xxx-xxxxx-x [DOCX]

Contents

Document Particulars

HP Records Document ID	D17/2132004		
HP Records Library ID	AD17/004088		
Version	0.8		
Content last updated	18/05/2021	Document status	FINAL
Document Classification	Official		
Due for review	July 2019		
Point of contact	s 22(1)(a)(ii)		
Approval Authority (EL2 or SES)	Executive Meeting		
Date of approval	04 September 2018		
NOTE: This is a controlled document in its electronic form only. Paper copies of this document are not controlled and should be checked against the electronic version prior to use.			

Document Review

This document's format should not be changed or appended to without consulting the document's owner - Director, Information Management, Technical Services Group.

Document is to be reviewed every 12 months or as required. The document particulars section is to be updated with a new review date once this document has been reviewed and updated as required.

Document History

Version	Date	Author	Summary of Changes	Status	Authorised by
0.1	4/12/2017	s 22(1)(a)(ii)		Initial Draft	s 22(1)(a)(ii)
0.2	22/01/2017	s 22(1)(a)(ii)	Minor changes	Draft	s 22(1)(a)(ii)
0.3	11/4/2018	s 22(1)(a)(ii)	Incorporated changes from consultation	Draft	s 22(1)(a)(ii)
0.4	10/5/2018	s 22(1)(a)(ii)	Review and update	Draft	s 22(1)(a)(ii)
0.5	15/06/2018	s 22(1)(a)(ii)	Feedback from DDP Committee	Draft	s 22(1)(a)(ii)

1.0	04/09/2018	s 22(1)(a)(ii)		Final	Executive Meeting
1.1	03/02/2020	s 22(1)(a)(ii)	Review to adopt DESE Branding	Final	Executive adoption of policy
1.2	03/03/2021	s 22(1)(a)(ii)	Update to Information to Systems Reckoner	Final	s 22(1)(a)(ii)

Purpose

The purpose of the Information Management Policy is to outline the department's requirements regarding the creation, ongoing management, and disposal of the official business information stored by The Department for its own and its client agencies use. The policy aims to ensure that all staff understand their individual obligations and accountabilities for information management; and that they can effectively:

- understand what official business information is
- identify useful or important information
- provide evidence of decisions, communications and activities
- meet accountability requirements and be able to demonstrate this
- support business activities through the creation of useable and reliable information, contributing to business efficiency and effectiveness
- provide accountability and ensure information remains available and accessible as long as it is required for operational and compliance purposes
- minimise business risk by ensuring the right information is captured to sustain business performance and continuity.

This policy replaces the department's Recordkeeping policy, which governed only records stored in official systems.

Related documents

This policy is supported by complementary policies, guidelines and procedures available from the department's Intranet > Information Management.

This policy should be read in conjunction with the following related documents:

- Information Management strategy 2017-2020
- Retention and Disposal Policy
- Information Security Policy
- Information Asset register (endorsed official information systems)

Policy Statement

The department will implement and practice robust information management procedures, and maintain fit for purpose systems to ensure the creation, maintenance and security of reliable information.

Information management practices in the department will be in accordance with this policy and it's supporting guidelines to promote best practice methods and deliver against the following official business information principles. Official business information is:

- Compliant: information management practices comply with legal and administrative requirements
- Reliable: information systems, procedures and practices work reliably to ensure that information is credible and authoritative
- Routine: when transacting business, information systems must be used in a manner that does not unreasonably impede business
- Retained: official business information is retained for as long as it is needed or is required to be kept
- Adequate and Complete: official business information must be adequate for the purposes it is kept, and contain not only the content, but also the structural and contextual information necessary to document a transaction.
- Protected: official business information must be stored and maintained securely in keeping with the requirements of the Information Security Policy, to prevent unauthorised access, destruction, alteration or removal and to meet privacy requirements.

Scope

In scope

This policy covers all forms of digital information managed by the department, and registered physical files (containing official business information) that are created by the Information Management Section.

Official business information:

- shows advice or instruction given
- shows decisions or recommendations
- provides contextual meaning to the information (usually contained in working documents)
- describes outcomes from meetings
- provides evidence of corporate administrative matters may be likely to be needed in the future.

All staff, including contractors and third parties who have access to, or create information for the department, are required to comply with this policy. The policy also covers all business applications used to create, manage and store information including official information management systems,

email, share files (network drives), websites, social media applications, databases and business information systems, regardless of security classification.

Unofficial information is:

- relevant only to the personal use of an individual user
- social, trivial or transitory in nature
- unaccredited, speculative, or does not inform a business purpose or provide any obvious business value to the department

s 22(1)(a)(ii)

Roles and responsibilities

Effective information management is dependent on the knowledge, skills, experience and attitudes of staff working in the department. Staff have various levels of responsibility when it comes to managing information depending on their role.

All employees and staff working in the department, including non-ongoing, contractor, consultant and service provider[1] staff are required to create and manage information as defined by this policy.

Managers and supervisors

- Ensure all staff are aware of, and are supported to follow, the information management practices defined in this policy.
- Advise the Information Management Section of any barriers to staff complying with this policy.
- Advise the Information Management Section of any changes in the business environment which would impact on information management requirements, such as new areas of business that need to be covered by a records authority.

Information Management Section

- Oversight of the management of information in the department consistent with the requirements described in this policy, and the department's IT Security Policy and Privacy Policy.
- Provide information management training, advice and general support to staff.

[1] Refer to the Records Management Instructions maintained by the Deeds Advice team, Quality and Integrity Group

- Develop and implement strategies to enable sound information management practices.
- Monitor compliance with information management policies and directives and advise senior management of any risks associated with non-compliance.
- Develop and maintain strategic documents for managing information management in the department.

ICT staff

- Develop and maintain the technology for business information systems, including appropriate system accessibility, security and backup.
- Ensure that any actions, such as removing data from systems or folders, are undertaken in accordance with this policy.
- Ensure that ICT systems support accountable and effective information management in consultation with the Information Management Section

IT Security Advisor

- Provide advice on security policy and guidelines associated with the management of information.

Senior Executive

- Champion and actively support and encourage adherence to this policy by promoting a culture of compliant information management within the department.

Secretary

- Ultimately responsible for ensuring there are robust management and security controls in place for the department's information.
- Champion, support and promote compliance with this policy
- Delegate responsibility for the operational planning and running of information management to the department's Chief Information Governance Officer (CIGO)

Creation and maintenance of information

Information must be created, maintained and stored to comply with this policy. Official business information must provide a reliable and accurate account of business decisions and actions; and include all necessary information to support ongoing business requirements and any review of advice, decisions or actions. This includes the names, dates and time, and any other key information required to capture the business context.

s 22(1)(a)(ii)

Systems used to maintain information

Information should be maintained and stored with other like information to provide contextual meaning. Information must be maintained in systems that ensure it is accessible by others, including information in draft, to account for events where the original author of the information is unavailable to share it or where documents require multiple collaborators.

The department manages and maintains its information digitally by default, in its original format, in order to preserve information integrity, version control and version history. Preferably, information is maintained in one repository or business system and that information is regarded as the source of truth. Information should ideally be retained in the system native to its origin, with the exception of email messages.

s 22(1)(a)(ii)

s 22(1)(a)(ii)

s 22(1)(a)(ii)

Destruction and transfer of information

The Archives Act mandates that information is disposed of in accordance with relevant records authorities. Advice must be sought from the Information Management Section before any disposal or transfer of the department's official business information. Unauthorised destruction of official business information must be reported by the department to the NAA for further action. Unofficial information can be destroyed under the Normal Administrative Practice (NAP) provision.

Further details are available from the Information Retention and Disposal policy

Appendix A: Legislation and compliance

The department is committed to complying with legislation, policies and standards relating to Information Management, including, but not limited to, the following artefacts:

Legislation, policies and guidelines

- Archives Act 1983

s 22(1)(a)(ii)

- Archives regulations

s 22(1)(a)(ii)

Appendix B: Glossary of Terms

Significant terms used in the Information Management Policy are defined or explained below.

Term	Definition
All staff	Those individuals or organisations who carry on the business of the department, including: • all department of Jobs and Small Business staff, including non-ongoing • staff • all contractors, and

	• all consultants and service providers engaged by the department.
Destruction	Process of eliminating or deleting information, beyond any possible reconstruction. Source: International Standard, ISO 15489, 2001, Part 1, Clause 3.8.
Disposal	Disposal of a Commonwealth record according to the *Archives Act 1983* means: • its destruction • the transfer of its custody or ownership, or damage or alteration.
Information retention	The retention period of information identifies the duration of time for which the information should be maintained or "retained", irrespective of format (paper, electronic, or other). Retention periods are determined based on content, regulatory requirements, involvement in litigation, reporting needs, as well as other factors as defined by local, regional, state, national and/or international governing entities.
NAA	National Archives of Australia
Official business information	Official business information includes that which: • shows advice or instruction given • shows decisions or recommendations • provides contextual meaning to the information (usually contained in working documents) • describes outcomes from meetings • provides evidence of corporate administrative matters may be likely to be needed in the future.
Records Authority	A records authority is a legal instrument that allows agencies to make decisions about keeping, destroying or transferring Australian Government records. They can also determine how long records need to be kept and arrange for their destruction after that time has passed.

Records Management Instructions	The Records Management Instructions (RMI) provides legally binding instructions on the management, retention and disposal of identified 'Records' created or used by organisations contracted by the Department of Employment (the department) under one or more of its Deeds.
Sensitive Information	When information is created, the originator is required to assess the consequences of damage from unauthorised compromise or misuse of the information. If adverse consequences from compromise of confidentiality could occur or the agency is legally required to protect the information it is to be given a protective sensitive marking.
Structured Information	Structured information is that can be easily ordered and retrieved e.g. database containing age, postcode.
Transfer	Change of location, custody, ownership and/or responsibility for information. Source: International Standard, ISO 15489, 2001, Part 1, Clause 3.20.
Unofficial business information	Unofficial business information is that not covered as official information. Unofficial business information can be disposal of by the creator without seeking formal authorisation from the Information Management section.
Unstructured information	Unstructured data has no identified internal structure e.g. Outlook emails, documents in the Shared Drive or SharePoint.
Working document	Data, computations, documents, drafts, records, rough notes, and sketches employed in the analysis or preparation of plans, projects, or other documents.

Australian Government
Department of Education, Skills and Employment

Information Retention and Disposal Policy

Contents

Document Particulars

HP Records Document ID	D18/8828		
HP Records Library ID	AD17/004088		
Version	0.6		
Content last updated	29 / 01 / 2019	**Document status**	**FINAL**
Document Classification	Unclassified		
Due for review	July 2019		
Point of contact	s 22(1)(a)(ii)		
Approval Authority (EL2 or SES)	Executive Meeting		
Date of approval	04/09/2018		
NOTE: This is a controlled document in its electronic form only. Paper copies of this document are not controlled and should be checked against the electronic version prior to use.			

Document Review

This document's format should not be changed or appended to without consulting the document's owner - Director, Information Management, Technical Services Group.

Document is to be reviewed every 12 months or as required. The document particulars section is to be updated with a new review date once this document has been reviewed and updated as required.

Document History

Version	Date	Author	Summary of Changes	Status	Authorised by
0.1	4/1/2018	s 22(1)(a)(ii)		Initial Draft	s 22(1)(a)(ii)
0.2	15/2/2018	s 22(1)(a)(ii)	Inclusion of backup information	Draft	s 22(1)(a)(ii)
0.3	11/4/2018	s 22(1)(a)(ii)	Incorporated changes from consultation	Draft	s 22(1)(a)(ii)
0.4	22/5/2018	s 22(1)(a)(ii)	Edits	Draft	s 22(1)(a)(ii)
0.5	23/5/2018	s 22(1)(a)(ii)	Updates	Draft	s 22(1)(a)(ii)
0.6	15/6/2018	s 22(1)(a)(ii)	Feedback from DDP Committee, Internal Audit	Draft	s 22(1)(a)(ii)

1.0	04/09/2018	s 22(1)(a)(ii)		Final	Executive meeting

Purpose

The purpose of the Information Retention and Disposal Policy is to outline the requirements for the Department of Education, Skills and Employment (the department) regarding the retention and disposal of all information stored by the department. The policy provides guidance for the department's staff to understand their individual obligations and accountabilities for the retention and disposal of information.

Policy Statement

Information is a key strategic asset and economic resource for the Australian Government. The department will manage official business information in accordance with relevant legislation and best-practice recordkeeping standards. This includes the:

- appropriate storage retention and disposal of digital information. All information retention and disposal practices in the department are to be in keeping with the requirements set out in this policy and supporting procedures (Information Management Policy and Information Security Policy)
- physical destruction of paper records
- erasing or purging email, documents or other data from business systems
- transfer of information to another agency as the result of machinery of government changes
- transfer to the National Archives of Australia (NAA).

Under the *Archives Act 1983*, 'Commonwealth records' cover all information in digital and non-digital formats that is created, used or received as part of government business. Therefore, all information belonging to the department, regardless of the system it is stored within, is subject to the requirements of the Act.

Additionally, the department is obliged to manage information in accordance with various legislation and regulations. A complete list of these is provided at **Appendix A – Legislation and Compliance.**

Scope

This policy applies to all information in any format and the associated metadata (or control records) stored by the department. It is inclusive of digital information holdings managed in business systems, and is not limited to information managed in information management systems.

Information considered in-scope includes:

- physical or digital documents
- paper or digital files (folders)
- production of reports or analysis drawn from data
- PDMS or PWS information
- department managed social media accounts– e.g. Twitter, Facebook, LinkedIn, blogs, wikis, discussion boards/forums

- web content – e.g. public websites, intranet, extranets, public websites and records of online transactions
- photographs
- data in business systems like databases and business information systems, shared folders, email applications, legacy systems and hard drives
- classified and unclassified information
- information stored in the production domain
- unstructured information – e.g. LAN drives, email, cloud based service offerings

Cabinet files (Sensitive: Cabinet) must be managed according to the guidelines provided in the Cabinet Handbook, and are out of scope of this policy.

All staff, including contractors and third parties who have access to, or generate information for the department, are required to comply with the policy. It further applies to organisations the department has outsourced its functions or activities to.

Backup requirements for all business systems must be considered, documented, approved and implemented. System owners must incorporate the requirements and decisions on data backup and retention into their as built system design documentation.

The Information Management Section will maintain an Information Asset Register. This is a listing of business systems that contain high-value, long-term information. Management of information in these systems must comply with the requirements of this policy.

Roles and responsibilities

Proper and lawful disposal of information is dependent on the knowledge, skills, experience and attitudes of staff in the department. Dependent on their role, staff have varying levels of responsibility when it comes to disposing of information.

All employees, including contractors, consultants and service providers[1]

- destroy non-official business information that falls within in the scope of Normal Administrative Practice

Managers and supervisors

- ensure staff, including contract staff, are aware of, and are supported to follow the information management practices defined in this policy
- advise the Information Management section of any barriers to staff complying with this policy

Information Management Section

- provide advice and support to the department in determining the correct retention periods for information
- provide advice on information to be disposed of to the department's Senior Executive
- provide final authorisation for the disposal of information after confirming all requirements have been met

[1] Refer to the Records Management Instructions maintained by the Deeds Advice team, Quality and Integrity Group

- monitor compliance with information management policies and directives issued by the NAA, and advise the department's Senior Executive of any risks associated with noncompliance
- maintain the Information Asset Register

ICT staff

- ensure information is disposed of in its entirety after being notified to do so by the Information Management Section
- ensure that any actions, such as removing data from systems or folders, is undertaken in accordance with this policy
- maintain data backups as directed to support business continuity and disaster recovery processes
- ensure the adequacy of existing processes to backup new systems and data, prior to production operation
- undertake periodic review of backup actions, to ensure backup arrangements are appropriate

Legal Services

- provide advice to the Information Management Section about any information that should not be disposed of for legal purposes

Senior Executives

- champion and actively support and encourage adherence to this policy by promoting a culture of compliant information retention and disposal within the department.
- authorise the disposal of information as recommended by the Information Management
- Section within the required timeframes

Secretary

- ultimately responsible for ensuring there are robust management and security controls in place for the retention and disposal of the department's information.
- champion, support and promote compliance with this policy
- delegate responsibility for the operational planning and running of information retention and disposal to the department's Chief Information Governance Officer (CIGO)

Information retention

The department will retain information in accordance with NAA approved Records Authorities[2] which give permission to the department to legally destroy or transfer information of their unique business activities. Records Authorities are issued by NAA under section 24 of the *Archives Act 1983*.

Official information must be retained in accordance with the retention periods defined in Records Authorities.

[2] For further information refer to NAA Records Authorities

Records Authorities

Agency-specific Records Authorities are issued to individual agencies by the NAA and specify retention periods and correct disposal actions for information and records of that agency's core business.

General records authorities are developed by the NAA and authorise the disposal of information and records of administrative business activities and responsibilities common to many Australian Government agencies. General records authorities cover information and records of business activities common to many agencies, including grant management or public and official inquiries, and set out the requirements for keeping, destroying or transferring that information.

The **Administrative Functions Disposal Authority** sets out requirements for keeping or destroying records of administrative business performed by most Australian Government agencies. This includes functions such as finance, human resources, procurement and publications management.

Digitising information

The department manages and maintains information digitally by default in its original format. It is appropriate to digitise information that holds value to the business of the department and is required to be retained for a reasonable period before it can be disposed. Information that is temporary in nature or due to be destroyed should be retained in physical format unless there is a specific business need to convert it. Once information has been digitised, quality assurance processes should be followed to ensure that the conversion is an accurate reproduction of the source (original) document.

For guidance on scanning requirements or quality assurance processes contact the Information Management Section.

In most circumstances, source documents can be destroyed legally[3] after quality assurance has been conducted, with the following exceptions:

- Permanent information created prior to 1 January 1980.
- Information which is subject to specific legal or administrative requirements such as:
    - legislation that requires retention of the original or source record in a specified form
    - government policy or directive not to destroy the original or source information
- digital original or source information which has been converted to paper or another physical format
- physical information that holds intrinsic value.

Retain information permanently

Selected official business information that has been determined as having continuing value is transferred to the NAA via the Information Management Section for permanent preservation and access. This is official business information that has been identified as Retain as National Archives (RNA) in a records authority, older than fifteen years and which is no longer used on a regular basis.

[3] Refer to NAA GRA 31 Destruction of source or original records after digitisation, conversion or migration

Metadata for official business information must be retained permanently in accordance with NAA's Administrative Functions Disposal Authority express Records Authority.

s 22(1)(a)(ii)

Information disposal

Information may be disposed after the specified minimum retention period has elapsed, or there is a requirement to transfer it out of the department.

On occasion, the NAA suspends its disposal permissions by issuing an information disposal freeze or retention notice. These override existing records authorities and prohibit the destruction of information related to certain events or circumstances until the freeze is lifted, or the notice is withdrawn. Current disposal freezes are listed on the intranet.

s 22(1)(a)(ii)

s 22(1)(a)(ii)

[4] This is in line with the revised NAA's AFDA Express retention authority

Appendix A: Legislation and compliance

The department is committed to complying with legislation, policies and standards relating to Information Management, including, but not limited to, the following artefacts.

Legislation, policies and guidelines

- Archives Act 1983

s 22(1)(a)(ii)

- Archives regulations

s 22(1)(a)(ii)

Appendix B: Glossary of Terms

Significant terms used in the Information Retention and Disposal Policy are defined or explained below.

Term	Definition
All staff	Those individuals or organisations which carry on the business of the department, including: • all Department of Education, Skills and Employment staff, including non-ongoing • staff • all contractors, and • all consultants and service providers engaged by the department.
Backup retention	The process of capturing critical business information for a period of time to insure against the loss of valuable information. The purpose of backups is to restore a system to a current state (as of the date of the most recent backup) in case of system failure, or to restore individual files inadvertently deleted or lost. Backup is not intended to serve as short or long term storage of information.
Destruction	Process of eliminating or deleting information, beyond any possible reconstruction. Source: *International Standard, ISO 15489, 2001, Part 1, Clause 3.8*.
Digitising	The process of converting information in physical format to digital format. For example, a paper record scanned and then saved as a digital record.
Disposal	Disposal of a Commonwealth record according to the *Archives Act 1983* means: • its destruction • the transfer of its custody or ownership, or damage or alteration.
Information retention	The retention period of information identifies the duration of time for which the information should be maintained or “retained”, irrespective of format (paper, electronic, or other). Retention periods are determined based on content, regulatory requirements, involvement in litigation, reporting needs, as well as other factors as defined by local, regional, state, national and/or international governing entities.
Metadata	Structured data or other information that describes context, content and structure of information and its management through time. It allows users to find, manage, control, understand or preserve the information it relates to. Source: *International Standard, ISO 15489, 2001, Part 1, Clause 3.12*.

Migration	Act of removing information from one system to another, while maintaining the information's' authenticity, integrity, reliability and use-ability. Source: *International Standard, ISO 15489, 2001, Part 1, Clause 3.13.*
NAA	National Archives of Australia
Official business information	Official business information includes that which: • shows advice or instruction given • shows decisions or recommendations • provides contextual meaning to the information (usually contained in working documents) • describes outcomes from meetings • provides evidence of corporate administrative matters may be likely to be needed in the future.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of authentic, complete and accurate information through time. Source: *International Standard, ISO 15489, 2001, Part 1, Clause 3.14.*
Records Management Instructions	The Records Management Instructions (RMI) provides legally binding instructions on the management, retention and disposal of identified 'Records' created or used by organisations contracted by the Department of Employment (the department) under one or more of its Deeds.
Soft Delete	To mark a record in a database for deletion or to temporarily prevent it from being selected. In order to actually delete the record, a "hard" delete or "permanent" delete function must be performed
Hard Delete	A permanent and unrecoverable deletion of a record in a database
Structured Information	Structured information is that which can be easily ordered and retrieved e.g. database containing age, postcode.
Transfer	Change of location, custody, ownership and/or responsibility for information. Source: *International Standard, ISO 15489, 2001, Part 1, Clause 3.20.*
Unofficial business information	Unofficial business information is that not covered as official information. Unofficial business information can be disposal of by the creator without seeking formal authorisation from the Information Management section.
Unstructured information	Unstructured data has no identified internal structure e.g. Outlook emails, documents in the Shared Drive or SharePoint.