Australian Government
Department of the Prime Minister and Cabinet

# Information Management Policy

Effective Date: 31 January 2017
v1.0



For Official Use Only

# Approval and Authorisation

## Owner

Name: s22

Title: Adviser, Records and Information Management

## Authorisation

This policy has been authorised by:

Elizabeth Kelly

Deputy Secretary, Governance
Chair, Information Governance Committee
Department of the Prime Minister and Cabinet

31/01/2017

## Production History

| Function | Date | Name/Comments |
|---|---|---|
| **Prepared** | June – August 2016 | s22 |
| **Reviewed** | September 2016 | Internal review and to Information Governance Committee (v0.9) |
| **Updated** | 21 September 2016 | Final comments incorporated into v1.0 |
| **Released** | 31 January 2017 | Final feedback incorporated and published |

## Release History

| Version | Name | Description | Approval | Date |
|---|---|---|---|---|
| **0.4** | Digital Transformation Office | DRAFT for information | Nathan Heeney | August 2016 |
| **1.0** | Information Governance Committee | FINAL for endorsement | Pat Sowry | January 2017 |

## Record Details

| | |
|---|---|
| **Number** | EDOC16/29260 |
| **ShareHub ID** | DOC16-70329 |
| **Location** | E15/262 |

# Contents

# 1 Overview

Information is a valuable resource of PM&C; it has real and measurable value. PM&C resources need to be carefully managed and information is no exception.

Information in the form of high quality advice is the core product we provide. Accurate, timely information is critical to effective decision-making at all levels of government. Further to this, there is an expectation that the collective information resources curated across the department are harnessed to benefit the government and ultimately, the Australian community.

This means PM&C must promote behaviours that value and carefully manage information to ensure it is timely, accurate and readily available when and where information consumers need it. This policy regulates PM&C's strategic imperative to organise departmental information and make it universally accessible and useful.

# 2 Scope

This policy applies to all PM&C staff, consultants, contractors and all aspects of the department's business operations, and includes any outsourced and other portfolio bodies with additional responsibilities according to their specific roles. This policy also applies to all PM&C business functions, capabilities or systems where information is created, captured, controlled, secured, managed, stored, preserved, kept, destroyed or transferred.

It is designed to be read in conjunction with documents identified in the Information Management Document Framework. (Annex 1)

# 3 Definitions and Abbreviations

| Term | Meaning |
|---|---|
| **APS** | Australian Public Service |
| **Classification** | The simple description of an information type. |
| **IM** | Information Management |
| **NAP** | Normal Administrative Practice |
| **PM&C** | (The Department of the) Prime Minister and Cabinet |
| **RIM** | Records and Information Management |
| **Security Classification** | A specialised form of classification that results in specific security related handling behaviours and the assignment of relevant security markings. |

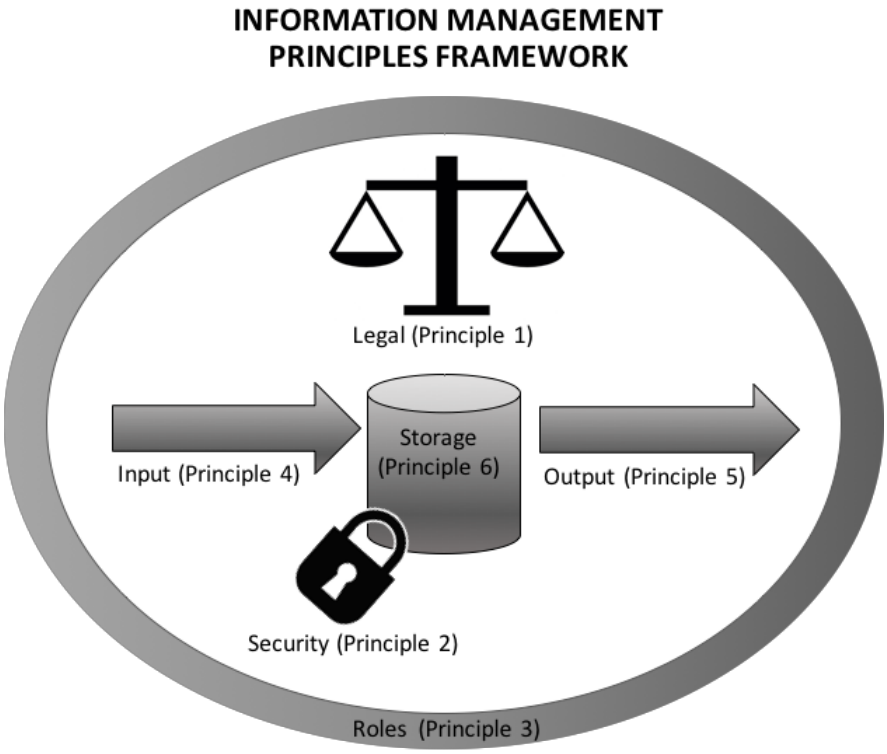
# 4 Principles and Implications

PM&C recognises that information is powerful and requires appropriate protection and management. The Information Management Principles contained in this policy guide PM&C in managing and using information appropriately. The overarching principles for Information Management at PM&C are:

1. Information is managed within the law (Legal)
2. Information is secure yet accessible (Security)
3. Information Management is a core staff competency (Roles)
4. Information is classified to increase utility (Input)
5. Information is easy to retrieve (Output)
6. Information architecture is designed for simplicity (Storage)

PM&C is committed to the principles and practices set out in whole-of-government policies and best-practice standards. These in turn are influenced by principles from the Australian Government Digital Continuity 2020 and Digital Transformation initiatives.[1]

The principles are designed to work together; they need to be applied to all PM&C initiatives or processes involving information. Excluding one or more principles will rapidly undermine PM&C's ability to supply information of consistent and measurable quality for decision-makers.




On occasion, principles may conflict and require resolution by PM&C information governance e.g. access considerations vs. security considerations. Initiatives involving information will not begin until they have been examined for compliance with these principles. If a conflict with any of the principles is found in a new or current initiative, then PM&C information governance will take the appropriate action.

[1] http://www.naa.gov.au/records-management/digital-transition-and-digital-continuity/index.aspx and https://www.dto.gov.au/

| Principle 1: Information is managed within the law (Legal) | |
|---|---|
| **Description:** | Information must be collected, stored, used, shared, disclosed and disposed in compliance with the legal and legislative requirements governing PM&C knowledge and information. |
| **What it means to me:** | "The information collected is legal"<br>"I understand my obligations"<br>"My privacy and the privacy of others is protected and safe" |
| **Rationale:** | PM&C must conform to all legal obligations, government mandated codes of behaviour and other legal provisions of confidentiality in the use of knowledge and information resources. This includes business process improvements that may lead to changes in policies and regulations.<br>This principle also means efficiency, need, and common sense are not the only drivers of Information Management.<br>PM&C must be, and be seen to be leaders in fulfilling legal obligations for information, setting an example of best practice for all government departments to follow. |
| **Implications:** | 1. Information must be acquired in a lawful manner.<br>2. Information must be controlled in terms of privacy and confidentiality.<br>3. Information must be appropriately classified and accessed.<br>4. Information must be managed under a defined lifecycle.<br>5. PM&C must put governance in place to ensure compliance with laws and regulations along with government policies regarding the collection, retention, and management of information.<br>6. Awareness through education along with access to legal and legislative requirements must be considered in the overall Knowledge and Information Management strategy.<br>7. Information collected must be "Fit for Purpose".<br>8. Changes in the law or regulations may drive changes in PM&C processes, applications and systems. |

| Principle 2: Information is secure yet accessible (Security) | |
|---|---|
| **Description:** | Balance information security requirements with the departmental need of information to be shared and accessible |
| **What it means to me:** | "I can trust that the data that I need to be secure is secure"<br>"I can and will protect sensitive information appropriately" |
| **Rationale:** | Open access to information and the release of information according to relevant legislation must be balanced with the need to adhere to security classifications protecting information.<br>The network separation of information and knowledge between PM&C Core and Indigenous Affairs still remains an overarching consideration which this principle is subject to. |
| **Implications:** | 1. Common methods and tools for creating, maintaining, and accessing information need to be adopted across the department.<br>2. PM&C will need to develop standard information models, elements, and other metadata that defines an accessible information environment and develop a repository system for storing this metadata to make it accessible.<br>3. Information accessibility will require a significant cultural change, and that cultural change will include opening up access, as well as a robust security culture.<br>4. The Information Governance Committee (IGC) will be responsible for overseeing PM&Cs requirements for highly classified systems.<br>5. Information should be shared where possible, in accordance with policies for secure sharing of information and "need to know" principles. |

| Principle 3: Information Management is a core staff competency (Roles) | |
|---|---|
| **Description:** | Staff clearly understand and execute their role in Information Management in a sustainable way. |
| **What it means to me:** | "I know why Information Management is important"<br>"I understand my role in Information Management"<br>"I will leave a legacy of good information practice"<br>"If I do Information Management right, everyone benefits, including me" |
| **Rationale:** | The success of IM lies in the ability of all the department to adopt effective IM practices. This means all staff have an important role to play.<br>People are more likely to readily adopt good practice when the reasons are clearly explained and they know how to apply it in their role. |
| **Implications:** | 1. Awareness and education is needed so all staff understand clearly why IM is important and how to apply it in their role as detailed in Annex 2. "Roles and Responsibilities"<br>2. Good IM needs to be clearly supported, articulated and modelled by department management.<br>3. Staff need to be developing IM in such a way so that after they leave, sustainable ongoing IM practices continue.<br>4. Relevant use cases and stories will be collected and broadcasted which highlight the difference and consequences of good and bad IM.<br>5. The handling of information within PM&C must be carefully designed and embedded in the 'business as usual' activities to avoid cumbersome or laborious processes. |

| Principle 4: Information is classified to increase utility (Input) | |
|---|---|
| **Description:** | PM&C will keep the information classification scheme as simple as possible |
| **What it means to me:** | "I can save my document quickly without overbearing red tape" |
| **Rationale:** | Classification of information leads to improved search capabilities for users which saves time and effort when finding information.<br><br>Increased utility means people will make greater use of information which in the long term improves information maturity across the department.<br><br>This principle is key to improving the ability of the department to fulfil strategic objectives by promoting effective information and knowledge management. |
| **Implications:** | 1. The classification scheme for information will be designed to be as simple as possible<br><br>2. PM&C recognises people are busy and therefore we need to make information classification easy whilst tracking and reporting on compliance.<br><br>3. Records management is undertaken in the background and is transparent to end-users utilising information systems. |

| Principle 5: Information is easy to retrieve (Output) | |
|---|---|
| **Description:** | Users have simple and effective access to the information needed to perform their duties. This means information is widely shared across departmental functions and divisions whilst still maintaining its security classification profile. |
| **What it means to me:** | "I can find my information easily"<br>"I can find other related documents without searching through pages of search results"<br>"Information is captured once and then linked to many times" |
| **Rationale:** | Ease of access to information leads to effective in decision-making since accurate and timely managed information is available to PM&C staff at all levels.<br>Easy retrieval enables timely response to information requests and opens the door to potential improvements in service delivery performance.<br>It is less costly to maintain single reliable versions of timely, accurate information which is easy to retrieve, than it is to maintain duplicate information in multiple systems. In addition to this, reuse is encouraged, information consistency is improved and time is saved by PM&C staff searching for information.<br>PM&C can be thought leaders for the rest of government in usage-based, demand-led approaches to information retrieval which fosters innovation and efficiency. |
| **Implications:** | 1. The retrieval and use of information must be considered from a department-wide perspective to promote use by a wider group authorised users.<br>2. PM&C will need to introduce a wide variety of search techniques along with usage tracking to drive continual improvement.<br>3. The way information is accessed and displayed must be flexible as to meet the needs of a wide range of users and methods of access.<br>4. Clear context, intent and definition for information must be developed and promoted in tandem with access and retrieval considerations.<br>5. Education is required to ensure that all parts of the department understand the value and importance of the easy retrieval of information. |

| Principle 6: The information architecture is designed for simplicity (Storage) | |
|---|---|
| **Description:** | There are as few applications per information sector as possible and as few information stores as possible. |
| **What it means to me:** | "I have just the right number of applications and each has a distinct purpose that I understand" |
| **Rationale:** | This principle provides guidance on how the application and information architecture of PM&C can be optimised to balance technology investment with the use of PM&C knowledge assets.<br><br>The network separation of information and knowledge between PM&C and Indigenous Affairs still remain an overarching consideration which this principle is subject to. |
| **Implications:** | 1. A design priority must be to consolidate knowledge into as few repositories as possible.<br><br>2. Potential reduced costs in business capability delivery as duplication is "designed out" of information, application and technology architectures.<br><br>3. PM&C must invest in software capable of migrating and integrating legacy information to realise a simplified information environment with easy retrieval and still continue to capitalise on significant investments in existing systems.<br><br>4. Enterprise wide information architecture policies and guidelines for owners and developers of new applications must be developed and promoted to ensure all information principles are upheld.<br><br>5. The information, application and technology architectures of PM&C must be designed to implement security requirements whilst promoting accessibility of PM&C information and knowledge. |

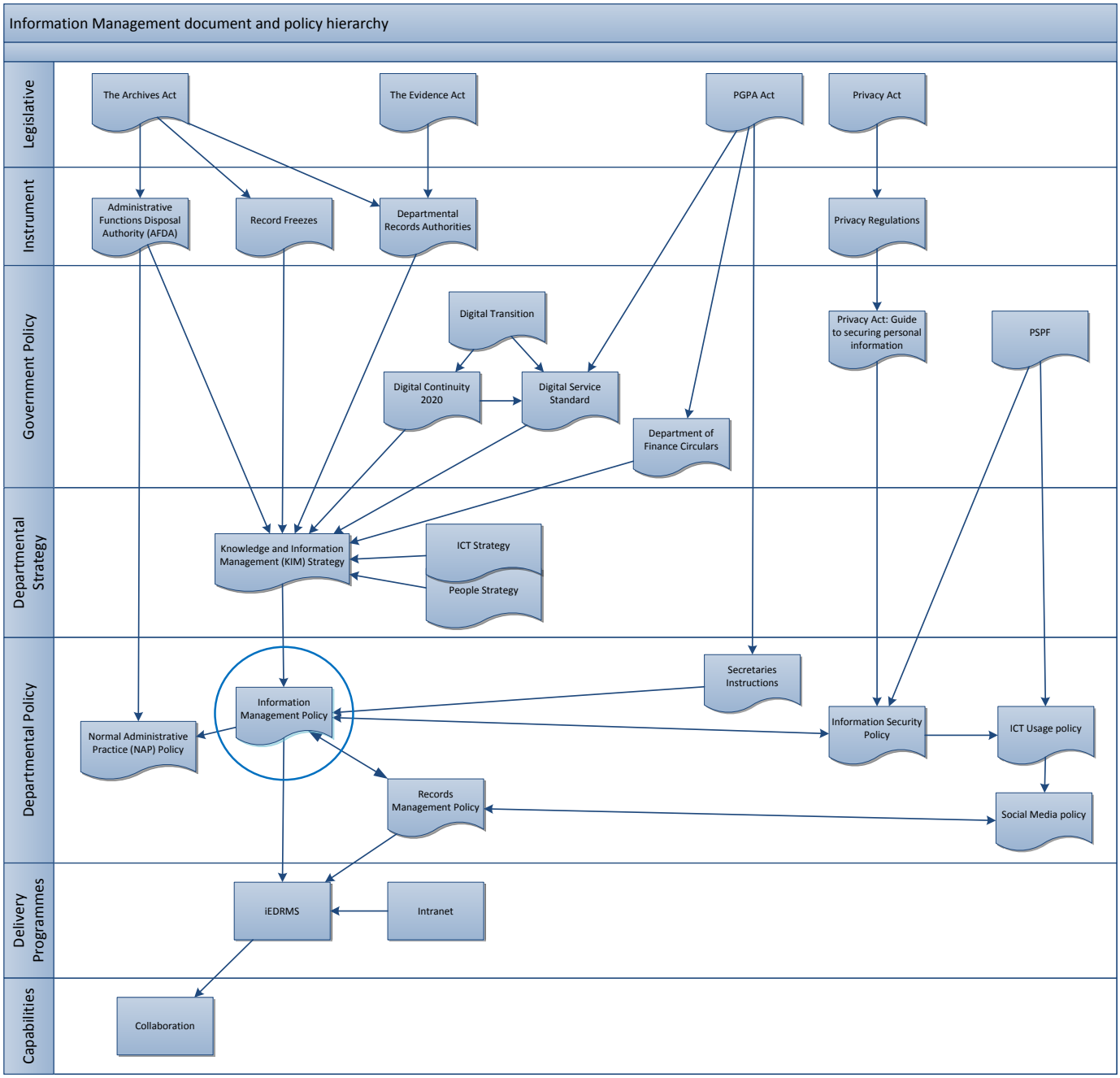
# 5 Authority

This policy is authorised by the Deputy Secretary Governance of the Department of the Prime Minister and Cabinet, and endorsed by the Deputy Secretary, Governance on 31/01/2017.

This policy constitutes a lawful direction made to staff under section 13(5) of the *Public Service Act 1999* to satisfy the legislative requirement for keeping and make records under the *Archives Act 1983*, and explain departmental performance under the *Public Governance, Performance and Accountability Act 2013*.

The authority for this policy comes from a suite of associated legislative and policy instruments (Annex 1). It also enables a number of other policies and strategies to implement the principles outlines.

# Annex 1. Information Management Document Framework




**Please note**: Information policy is at the very heart of an open and transparent governance structure. There are many legislative and policy directives that aim to ensure good governance and practice across the APS. The diagram above is only an abridged representation. For more information please refer to the National Archives of Australia who have a dedicated page describing the obligations in detail.

# Annex 2. Roles and Responsibilities

### 5.1.1 The Secretary of PM&C

- **authorise** the IM policy
- **authorise** the RIM Director to decide recommendations on the destruction of information
- **provide** sufficient support and resources for ensuring a successful IM program is delivered
- **create** a new PM&C value for the promotion and demonstration of genuine participation in the performance management scheme and better practice IM
- **promote** compliance with PM&C IM policies and procedures, and
- **promote** the exchange of information within PM&C and more broadly across the APS.

### 5.1.2 The Director responsible for IM

- **ensure** that PM&C's IM practices comply with its obligations and responsibilities as a Commonwealth agency
- **develop** strategies to ensure PM&C establishes itself as a site of best practice IM
- **oversee** and support the IM functionality of PM&C's information systems
- **develop** strategies to ensure all staff are aware of PM&C's IM requirements and the IM policy
- **create** and maintain IM procedures documenting PM&C's IM requirements and containing IM rules and practices that all PM&C employees are obliged to follow, and
- **review** PM&C's IM systems.

### 5.1.3 Records and Information Management staff

- **promulgate** PM&C's IM policies and procedures to all staff
- **monitor** staff compliance with the IM policy
- **deliver** IM training and advice to all staff
- **maintain** and monitor PM&C's IM systems, and
- **ensure** that information is kept only as long as PM&C, government and the public require them, as established by Records Authorities.

### 5.1.4 ICT staff, including system administrators

- **maintain** the technology used to support systems that capture and keep information electronically, ensuring the systems are reliable, available and accessible to staff for as long as the systems are required
- **seek** IM plan as part of any system commissioned development
- **seek** out standardised methods that are easily employed and compatible with existing IM systems, and

- **promote** and reuse the information contained within their information systems in accordance with this policy.

### 5.1.5 All managers and supervisors of PM&C employees

- **monitor** staff under their supervision to ensure staff understand and comply with PM&C IM policies and procedures for the creation and maintenance of records, and
- **support** and foster a culture within their workgroup that promotes good IM practices.

### 5.1.6 All employees of PM&C, including contractors

- **understand** the IM obligations and responsibilities that relate to their position.
- **ensure** that reliable and useable information is created, managed, protected and retained for respective retention periods.
- **adhere** to organisational policies, procedures and standards in keeping records documenting their daily work, and specifically create and capture information into identified IM systems for the following business activities:
    - approval or authorisation
    - guidance, advice or direction
    - information relating to projects or activities being undertaken
    - formal business communications between staff and external recipients
    - formal business communications between staff, and
- **only destroy** information under an authorised Records Authority or through the application of PM&C's NAP policy with authority of the RIM Director.

### 5.1.7 The Agency Security Adviser

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

### 5.1.8 PM&C information owners

- **promote** their information catalogue so the information is available to staff who require access to the information in the course of their duties.

### 5.1.9 Staff procuring consultants or contractors

- **ensure** that contracts with consultants or contractors explicitly state the ownership of all information created, captured or published during the course of their work with the department resides with PM&C
- **educate** consultants or contractors covering the creation, management, access to and destruction of information

Australian Government
Department of the Prime Minister and Cabinet

# Records and Information Management Team

## Records Management Policy

**Effective Date: March 2014**
**V1.2**

# Approvals

## Owner

Name: Records and Information Management Team

## Authorisation

Name: Elizabeth Kelly

Title: Deputy Secretary, Governance

## Release History

| Version | Name | Description | Approval | Date |
|---|---|---|---|---|
| 1.0 | Information Services Branch | Created in consultation with Divisions and Executive | Dr Peter Shergold | October 2005 |
| 1.1 | s22 | Privacy Act Reforms | Elizabeth Kelly | February 2014 |
| 1.2 | s22 | Changes made to reflect transition to electronic records management | Elizabeth Kelly | March 2014 |

# 1 Preliminaries

## 1.1 Purpose

The purpose of this policy is to provide a framework for the effective creation, capture, and management of records within the Department of the Prime Minister and Cabinet.

This document contains guidelines and practical advice on a broad spectrum of internal records management practices and issues. Together with the Chief Executive Instruction (CEIs) - Chapter 11, this policy aims to provide specific details of what records must be kept, how they must be stored and managed, and how they should be shared and used within the Department.

## 1.2 Scope

This policy covers the management of records including physical and electronic records, documents, data, and web resources gathered, created, or retained by employees in the performance of their duties within the Department of the Prime Minister and Cabinet.

This policy does not cover the systems used to manage specialised records including Cabinet and Executive Council records, personnel, and finance records, nor do they take precedence over the specific handling requirements for the management of intelligence material.

While the general principles of records management detailed in this policy still apply to these systems, their specific operation are not considered within the scope of this document.

## 1.3 Authorisation

The Records Management Policy for the Department of the Prime Minister and Cabinet was originally authorised by the Secretary, Dr Peter Shergold.

## 1.4 Compliance

All employees of the department including staff, consultants and contractors must comply with the mandatory policy statements and procedures outlined in this policy. These statements are drawn from the Chief Executive Instructions and carry the force of law.

## 1.5 Document Authorship

The Records Management Policy has been developed by the Business Services Branch in consultation with Divisions and Executive.

This policy incorporates existing National Archives policies and material from the “Keep the Knowledge – Make a Record” publications, to ensure they reflect common and consistent language and concepts of recordkeeping across Australian Government.

Any questions regarding the application of this policy should be directed to the Records and Information Management Team.

## 1.6 Review

This policy will be reviewed annually or as required to reflect changes in the broader Australian Government legislative and regulatory environment, best practice standards, and to ensure currency and relevancy to the business of the Department.

## 1.7 Relationship with other Policies

This document contains policies, guidelines and practical advice on a broad spectrum of internal information and records management practices and issues. It covers some areas in more detail than others as there are already complementary policy and guideline documents available in the Department including the IT and Internet Usage Policy, Information Security Protocol, and the Protective Security Policy Framework (PSPF).

## 1.8 References

Where instructions or guidelines are referenced throughout this document hyperlinks have been provided to the relevant documents on the Department's Intranet.

Summaries of the relevant legislation governing the creation, use, and management of records are provided in Appendix 2.

# 2 Introduction

## 2.1 Why is good Recordkeeping Important?

Good recordkeeping is an essential requirement for efficient government administration and accountability. It is the basis for establishing and maintaining documentary evidence of government activities and helps agencies manage and preserve corporate memory for short and long-term purposes.

### 2.1.1 Organisational Accountability

As an Australian Government department we are responsible and accountable to the Government and the public for our actions as individuals and as an organisation. The Department needs to be able to demonstrate the effective, efficient, and ethical use of resources and be accountable for decision-making processes in accordance with the law.

Records show whether the Department, or responsible individuals within it, have met defined legal, organisational, social, or moral obligations. We therefore need to keep accurate account of our business activities through good information management, recordkeeping and document management practices. Anything that documents or provides evidence of the Department's business needs to be kept as a record. These records must be created in a way which makes it possible to prove that they are what they purport to be, that they are accurate, authentic, have integrity, and are irrefutable.

### 2.1.2 Delivering Better Outcomes

Not only are Commonwealth agencies required to carry out their business in an accountable, equitable, and efficient manner but there is increased scrutiny on the quality, robustness, and innovation of programmes and services delivered by government.

The primary function of the Department is the provision of effective, sound, and well-coordinated advice and support services to the Prime Minister and Cabinet.

Good information management through effective recordkeeping supports all communication and decision- making. It is essential to delivering accurate, innovative, and robust policy advice and in ensuring the advice and services the Department provides are timely and effective. We need access to up-to-date and accurate research and data, but also an understanding of past decisions, policies, and activities to provide a sound base for supporting future policy analysis and decision-making.

## 2.2 How to use this Document

Together with the Chief Executive Instructions (CEIs) these guidelines provide a framework for the effective creation, capture, and management of records within the Department. They outline what records must be kept and how they must be stored and managed to ensure that they are used effectively in achieving the Department's objectives while retaining their value over time.

While these documents include mandatory policy statements to which all employees must comply, they provide flexibility where possible, to allow each work area or team to develop their own work practices relevant to the nature of their business or to their work preferences.

# 3 Authority

There are a number of Acts and standards that govern the creation, capture, use, management, archiving and destruction of Commonwealth information and records. The Department is committed to developing information management and recordkeeping policy and processes that meet the requirements of its legislative and regulatory environment as well as the best practice standards recommended in the Australian Standard for Records Management (AS ISO 15489).

All employees with responsibilities for managing information and records must comply with relevant laws and standards in the creation, use and management of Commonwealth records and information. All records, regardless of format, must be managed in accordance with the *Archives Act 1983* and both information and records are subject to related legislation such as the *Electronic Transactions Act 1999*, the *Evidence Act 1995*, the *Freedom of Information Act 1982* and the *Privacy Act 1988*.

## 3.1 In Practice

You should be aware of the intent of the key legislation governing the management of information and records as outlined in Appendix 2 - Legislative and Regulatory Obligations. You should also be familiar with and comply with the Chief Executive Instructions - Chapter 11 and this policy which has been developed to comply with these laws in the specific business context of this Department.

# 4 Policy

## 4.1 Statement

All information that you receive or create in the performance of your official duties is a Commonwealth information resource and is subject to the legal obligations for managing information outlined in Appendix 2. Where this information provides evidence of the substantive business activities of the Department, these resources are also Commonwealth records and must be managed in accordance with the specific legislative requirements and standards which govern recordkeeping.

The key distinction between records and other types of information is that records provide evidence of business activities. They document what we do as Commonwealth employees whether we are preparing briefs, developing policy, answering a ministerial or undertaking more operational activities such as recruitment and financial management. They capture our decisions, actions, consultations, communications, transactions and outputs.

### 4.1.1 In Practice

A significant amount of the information you create and deliver as part of the business objectives of the Department and its role in supporting government is evidence of the Department's function in government and must be treated as Commonwealth records. You are responsible for retaining documents and information which provide evidence of your work activities including business decisions, consultations, communications and transactions and for ensuring that they are stored and managed effectively and efficiently as Commonwealth records.

In some cases this may also include information that has been gathered from external sources, particularly where this has been used as the basis or justification for the decision or actions outlined above.

It is sometimes difficult at the point when you are undertaking day-to-day activities to see the continuing value of the records you create. However, it is often only after the event, when you might need to explain the reasoning behind certain actions or you need to understand decisions made by others, that a complete history of a subject or activity is useful.

## 4.2 What is recordkeeping?

Simply keeping records in filing cabinets, drawers, or in electronic directories is not sufficient to ensure that they can be used to account for, or provide official evidence of your activities or actions. Without this evidence, the Department cannot meet its legal obligations of accountability and transparency to the Australian public and the government it serves.

For records to be able to be used in evidence the Department must be able to substantiate that they are a true record, that they are an accurate and complete representation of what has occurred and that they have not been altered. Recordkeeping is the formal practice of organising, structuring, categorising, cataloguing, and tracking of records in a centralised and controlled approach. Recordkeeping systems (whether electronic or paper-based) provide the additional intellectual and physical controls around records that allow them to be used as evidence.

The structured grouping of records by subject or activity also ensures that the relationship between the individual records or documents is clear so that the history and development of ideas or the order of actions or decisions can be ascertained.

### 4.2.1 In Practice

You are responsible for making sure that the records which you create or receive are registered and managed in the appropriate departmental recordkeeping system. These records should enable you to explain or justify what you have done, show the extent of your responsibility for decisions taken and show the order of events and your role in them.

## 4.3 The Department's Recordkeeping System

The Department's official recordkeeping system is HP Records Manager (HP RM) and it is used for the management of both electronic and paper records. The system is used to register and track the existence, location, and status of records to facilitate access, retrieval, archiving, and disposal.

There are other systems in use in the Department for specialised records including Cabinet records, personnel and finance records. While the general principles of records management detailed in these guidelines still apply to these systems, their specific operation are not considered within the scope of this document.

## 4.4 Record Formats

Records can be in a variety of formats, and can include: emails, letters, CDs, USB drives, posters, maps, reports, and plans.

As the tools we use to create and deliver information have changed, our understanding of what a record looks like has changed. We create and share the majority of our information via electronic means and this has fundamentally changed the way we need to view and manage our records. Records are no longer only contained in traditional physical formats such as documents, letters, and publications. Increasingly, records are also being created in formats where the record would lose its original integrity outside of the medium in which it is delivered. For example, websites are constructed of multiple graphic and text files which individually do not show the relationship of the information as it was presented on the site. Another example is records created in other media formats such as audio, audio-visual and photographic media.

The Department has provided a recordkeeping system that is able to manage different electronic formats and therefore support the creation and capture of electronic information in order to support business requirements.

# 5 Responsibilities

The responsibility for good recordkeeping does not only rest with records management staff, divisional support staff, and managers. It is a responsibility of all staff to ensure records are created, captured, used and stored in accordance with the principles and practices explained in this policy.

Outlined in this chapter are the broad responsibilities associated with specific roles.

## 5.1 All Staff

All employees are accountable for the efficient, effective and appropriate use, management and security of records and information resources that are received, created, acquired or retained in the performance of official duties.

| Role | Responsibilities |
|---|---|
| Staff | All employees have an individual responsibility to make themselves aware of and comply with the Records Management Policy including:<br>• Creating complete, meaningful and accurate records of their work-related activities.<br>• Capturing these records into the Department's recordkeeping system.<br>• Understanding and applying the security requirements of the records in their care in accordance with the Information Security Protocol.<br>• Understanding the additional recordkeeping obligations related to their specific role or position as detailed in this policy. |

*Contractors and consultants undertaking work for the Department are subject to the same guidelines as other staff and must be familiar with and comply with the Department's policy and guidelines on the management of information and records.

## 5.2 Corporate Responsibilities

### 5.2.1 The Chief Executive

The Chief Executive of each government agency is responsible under the *Public Governance, Performance and Accountability Act 2013* for managing the affairs of the Department in a way that promotes efficient, effective and ethical use of Commonwealth resources.

| Role | Responsibilities |
|---|---|
| The Chief Executive | The Chief Executive is responsible for ensuring that adequate records are created and maintained by:<br>• Appointing an Assistant Secretary to coordinate the delivery of information and records management services and operations.<br>• Advocating the management of information and records as a strategic resource and ensuring management of information considerations are taken into account in all Departmental plans and activities.<br>• Supporting and engendering a culture within the Department that recognises and values good records management practices.<br>• Allocating appropriate and adequate resources to the records management functions and operations in the Department.<br>• Ensuring that records management policies standards, guidelines, and procedures are established and that governance mechanisms are in place to ensure compliance with obligations. |

### 5.2.2 Records and Information Management

The records and information management group consists of the Assistant Secretary Business Services Branch, Library Records and Information Management Section, and the Records and Information Management Team.

| Role | Responsibilities |
|---|---|
| Assistant Secretary Business Services Branch | The Assistant Secretary is responsible for ensuring:<br>• All information management strategies, policies, services, and operations are integrated and support both the business needs of the Department and reflect the Government's Information Management and IT strategic priorities.<br>• Ongoing development and improvement of cost effective strategies and tools designed to maximise the effective use of information resources by the Department in achieving its business and strategic objectives. |
| Library, Records, and Information Management Section | The Library Records and Information Management Section is responsible for:<br>• Providing advice and practical strategies to better integrate information and records management policy, practices and support.<br>• Ensuring that policies and procedures are developed, reviewed and updated in accordance with relevant legislation and Commonwealth recordkeeping requirements and promulgated to all staff. |

| Role | Responsibilities |
|---|---|
| Records and Information Management Team | The Records and Information Management Team is responsible for:<br>• Establishing a records management program to ensure that records are properly protected and managed in a way that supports their use for accountability and information resource requirements.<br>• Ensuring that procedures and practices are implemented in accordance with Departmental policy.<br>• Providing education, advice and support to all staff aimed at improving the efficiency and effectiveness of recordkeeping.<br>• Identifying vital records and establishing records disaster and recovery plans to ensure business continuity.<br>• Administering the Department's file management system, HP RM.<br>• Providing support to localised records support staff. |

### 5.2.3 Managers and Supervisors

| Role | Responsibilities |
|---|---|
| Managers and Supervisors | In addition to their individual responsibilities to understand and comply with the Records Management Policy all managers and supervisors are also accountable for the effective management of information and records in their work area. Regardless of their level they are responsible for ensuring that:<br>• New starters in their work unit (Division, Branch, Section or team) are made aware of the Department's expectations and guidelines about the use and care of records in the first week of their duties.<br>• Staff, consultants, and contractors under their direct supervision understand and comply with these guidelines.<br>• Staff under their supervision have the time, resources, and training opportunities to enable them to meet their individual responsibilities outlined in these guidelines.<br>• Performance agreements made with staff articulate recordkeeping responsibilities and performance measures.<br>• Staff under their supervision only have access to records consistent with their security classification and in accordance with the 'need to know' principle. |

### 5.2.4 Localised Records Support Staff

| Role | Responsibilities |
|---|---|
| Localised Records Support Staff | Staff who manage independent file management systems either for the purposes of managing secure records or other record series are responsible for coordinating with the Records and Information Management Team in managing these records to ensure compliance with departmental policy. |

# Appendix 1 – Glossary

| Term | Definition |
|---|---|
| **B** | |
| Business Activities | All the functions, processes, activities and transactions of an organisation and its employees. This includes public administration as well as commercial business. Australian Standard for Records Management (AS ISO 15489) |
| **C** | |
| CEIs | Chief Executive Instructions. |
| Commonwealth Records | All recorded information, regardless of medium or format, created or received by an agency or its agents under Commonwealth law or in connection with the transaction of public business which are preserved because of their continuing administrative, legal, financial, or informational value or their enduring archival value. |
| Corporate Information | All documents, publications, data and other information that is created, gathered or received by the Department in its operations. |
| Corporate Records | All corporate information which is evidence of the business of the Department including decision, actions, transactions, communications and outputs. |
| Corporate Repositories | Corporate systems that have been designed to control and manage corporate information, data or records in a secure and controlled environment. |
| Custodian | An official responsible for the safe use, proper custody, security and maintenance of corporate information and records. All officials are considered custodians for the purposes of the Chief Executive Instructions. |
| **D** | |
| Database | Integrated data files organised and stored electronically in a uniform file structure that allows data elements to be manipulated, correlated, or extracted to satisfy diverse analytical and reporting needs. |
| Departmental File | An official container used to hold and protect a group of like records of the same medium or physical type e.g. paper, compact disc, video, photographs.<br>Departmental files are created by the Records and Information Management Team and are entered into the records management system at the point of creation to facilitate retrieval, tracking, and disposal. |
| **E** | |
| Electronic Records | Any information that is recorded in a form that only a computer can process and that satisfies the definition of a record. |
| EDRMS | Electronic Document and Records Management System |

| Term | Definition |
|---|---|
| Employees | All personnel employed by the Department of the Prime Minister and Cabinet or working on secondment or placement in the Department. This includes all permanent and non-ongoing staff, consultants and contractors. |
| Evidence | Information that tends to prove a fact. It is not limited to the legal sense of the term. |
| **F** | |
| File Name | The name given to electronic documents, spreadsheets and other data formats when they are saved. |
| **M** | |
| Metadata | Data describing data and data systems. Information that is used to facilitate intellectual control of, and structured access to, other information. |
| **P** | |
| Personal Information | Documentary materials or correspondence that is of a private or non-public nature, that relates solely to an individual's own affairs that do not relate to or have any effect upon the conduct of the Department's business. |
| **R** | |
| Records | Records are the information, regardless of format or media, created, received, or maintained by employees in the course of the Department's business which are evidence of business activities and transactions as well as the associated actions, decisions, outputs, and outcomes. |
| Recordkeeping | The process of creating and maintaining complete, accurate, and reliable evidence of business transactions in the form of recorded information. |
| Recordkeeping Systems | A manual or automated system which provides a mechanism for the reliable and systematic control and management of records to ensure the effective capture, management and access to these records over time. |
| **S** | |
| Staff | See Employees |

# Appendix 2 – Legislative and Regulatory Obligations

## Key Legislation Governing Recordkeeping

| Act | Description |
|---|---|
| *Archives Act 1983* | The *Archives Act 1983* officially established the National Archives of Australia. The Act empowers the Archives to preserve the archival resources of the Commonwealth (those records designated 'national archives') and defines their role in supporting and governing the creation and management of these records. More importantly the Act establishes the framework in which agencies must create, capture and manage their records including:<br>• Imposing statutory obligations on all Government departments and agencies for the management of their records.<br>• Making it illegal to destroy or alter Commonwealth records without the permission of the Archives, unless otherwise stated by law.<br>• Creating a fundamental right of public access to records over 30 years old and allowing for provisional access to those less than 30 years old.<br>• Governing the retention and disposal of records to ensure:<br>o identification and preservation of those records which must be kept permanently as part of the archival resources of the Commonwealth; and<br>o efficient and economical recordkeeping in the Australian Government - including the prompt destruction of records no longer needed for business purposes. |

# Other Legislation Affecting Commonwealth Records

| Act | Description |
|---|---|
| *Electronic Transactions Act 1999* | The *Electronic Transactions Act 1999* provides a regulatory framework that enables business and the community to use electronic communications in their dealings with government. The primary objective of the Act is to remove impediments that might prevent a person from using electronic communication to satisfy obligations under Commonwealth law.<br><br>Broadly, the Act provides that electronic communications and electronic forms of documents may be used to satisfy requirements or permissions, under Commonwealth laws, for a person to:<br>• give information in writing<br>• provide a signature<br>• produce a document that is in the form of paper or other material<br>• record information in writing<br>• retain a document that is in the form of paper or other material, or<br>• retain information that was the subject of an electronic communication<br><br>The Act provides for exemptions and it identifies conditions that must be met in order to maintain the integrity and accessibility of information. |

| Act | Description |
|---|---|
| *Evidence Act 1995* | The new *Evidence Act 1995* recognises the role of modern technologies in business and government. It abolishes the 'original document' rule and ensures that faxes, telexes and electronic communications may be admitted into evidence in all federal courts.<br><br>The Act contains a new definition of a 'document'. A document is defined as:<br><br>'anything on which there is writing, anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them or anything from which sounds, images or writings can be reproduced with or without the aid of anything else.'<br><br>If the document in question is an 'article or thing on or in which information is stored in such a way that it cannot be used by the court unless a device is used to retrieve, produce or collate it', it is permissible to tender 'a document that was or purports to have been produced by use of the device'.<br><br>To be admissible the record must be:<br>• authentic - it must be clear that the record or document has not been altered or modified without authority<br>• complete and accurate; and<br>• logically sequenced and arranged. |

| Act | Description |
|---|---|
| *Freedom of Information Act 1982* | The *Freedom of Information Act 1982* (FOI) governs public access to documents kept by Australian Government departments. The objective of the Act is to extend as far as possible the right of the Australian community to obtain access to information in the possession of the Australian Government by requiring agencies to:<br>• publish information about their operations and powers affecting members of the public, and<br>• provide access to documents in their possession unless the document is within an exception or exemption specified in the legislation.<br>Members of the public have a right to:<br>• access information about the operations of departments and public<br>• authorities, in particular information about the rules and practices which may affect them<br>• access documents in the possession of Ministers, departments and public authorities unless they are exempt to protect essential public interests, private or business information, and<br>• request amendment of records containing personal information which are incomplete, incorrect, out of date or misleading; and<br>• appeal decisions.<br>The FOI Act sets out certain documents that may not be accessed (exempt documents). Generally, these documents are those which must be kept confidential to protect essential public interests, personal or business information.<br>The Access and Administrative Review Section in Government Division coordinates the processing of the Department's FOI requests and provides advice and assistance. Further information is available in the Guide for FOI Decision-Makers. |
| **Act** | **Description** |
| Privacy Act 1988 | The *Privacy Act 1988* provides protection to individuals against the mishandling of personal information by Australian, ACT and Norfolk Island government agencies and certain private sector organisations. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether that information is true or not and whether it is recorded in a material form or not.<br>The Australian Privacy Principles set out standards, rights and obligations in relation to the handling and maintenance of personal information, including dealing with privacy policies and the collection, storage, use disclosure, quality and security of personal information and access and correction rights of individuals in relation to their personal information. |

## Other Standards, Authorities, and Related Legislation

| Regulation/ Standard | Description |
|---|---|
| *Crimes Amendment Act 1982* | The *Crimes Amendment Act 1982* contains provisions regarding the unlawful disclosure of information and the falsification of financial information and records. |
| *Public Governance, Performance and Accountability Act 2013* | The *Public Governance, Performance and Accountability Act 2013* requires that Chief Executive Officers (CEOs) manage the affairs of their agency in a way that promotes proper use (that is, efficient, effective and ethical use) of the Commonwealth resources for which they are responsible. |
| *Public Service Act 1999* | Under the *Public Service Act 1999*, the Australian Public Service (APS) is 'openly accountable for its actions, within the framework of ministerial responsibility to the Government, the Parliament and the Australian Public'. Under directions issued by the Public Service Commissioner pursuant to the Act, both Agency Heads and APS Employees are obliged to take reasonable steps to ensure that they understand and operate within the government's accountability framework.<br><br>The Commissioner identifies that an agency's ability to 'demonstrate that due process has been followed in its actions and decisions… through the existence and maintenance of good record keeping systems' is an effective indicator of compliance with this regard.[1] |
| *Australian Standard For Records Management:*<br><br>*AS ISO 15489* | The Australian Standard for Records Management (AS ISO 15489) provides strategies and operational guidelines for the implementation of records management practices and procedures in any organisation. The Standards are designed to help organisations create, capture and manage full and accurate records to meet their business needs and legal requirements as well as to satisfy other stakeholder expectations. They apply to records in any format or media, created or received by any public or private organisation during the course of its activities. |

[1] Public Service and Merit Protection Commission, Values in the Australian Public Service, 2002

| Regulation/ Standard | Description |
|---|---|
| National Archives of Australia – General Disposal Authority 25 - A guideline for agencies about their responsibilities for recordkeeping in outsourcing arrangements. | General Disposal Authority 25(GDA 25) covers the transfer of custody and ownership of records to contractors providing services on behalf of or to government under outsourcing arrangements. The authority is incorporated in Records Issues for Outsourcing which provides guidelines for agencies about their responsibilities for recordkeeping when employing contractors.<br>This guideline has three purposes:<br>• to assist officers involved in the decision making process identify and address records issues when outsourcing service delivery or support services<br>• to authorise the transfer of custody or ownership of records to a contractor, as required by the *Archives Act 1983*, and<br>• to provide details of other sources of information which are relevant to records issues.<br>The guideline consolidates information about records currently available from a number of sources.<br>It addresses three categories of records:<br>• those held by the agency prior to the commencement of the contract<br>• those created and maintained by the contractor, and<br>• those created by the agency during the course of the contract. |
| National Archives of Australia – General Disposal Authority for source records that have been copied or migrated. | General Disposal Authority for Source Records that have been Copied, Converted or Migrated permits agencies to destroy a range of source records that are no longer needed once they have been copied, converted or migrated, provided equivalent reproductions are maintained and there are no special requirements to retain the source records. It also sets conditions for the proper management of copying, conversion and migration processes, the reproductions that are generated through those processes, and the source records themselves. The GDA for source records both replaces and expands the coverage of GDA No. 22, which applied only to records of short-term value that had been copied. |

## Department Specific Guidelines

| Other Guidelines | Description |
|---|---|
| Cabinet Handbook | Maintaining the confidentiality of the Cabinet's deliberations requires special arrangements to be made for the handling of Cabinet documents. Cabinet records are maintained as a separate series and are maintained as the property of the Commonwealth rather than of individual ministers or departments. |

**ATTACHMENT A – NAP POLICY**

Australian Government

Department of the Prime Minister and Cabinet

# Normal Administrative Practice (NAP) Policy

**Document Author:** Records Management Unit

**Published:** 19 December 2011
**Last Updated:** 17 April 2018

Australian Government

Department of the Prime Minister and Cabinet

# NORMAL ADMINISTRATIVE PRACTICE (NAP) POLICY

**Contents** **Page No**

## 1. PURPOSE

This policy provides a framework for the application of a 'normal administrative practice' (NAP), set out in section 24 (2) (c) of the *Archives Act 1983*, to guide the routine destruction of the records that are not needed as evidence of the department's business, and do not form part of its corporate records.

## 2. POLICY STATEMENT

The Department of the Prime Minister and Cabinet's records are a key component of its corporate memory and as such are vital assets that support the ongoing operations of the department. They provide clear evidence of business activities over time. The department is committed to implementing and supporting good records management practices to ensure creation, maintenance, protection, appropriate retention, and/or accountable destruction of its records that are conducted in accordance with the regulatory requirements of a Commonwealth agency under the *Archives Act 1983*.

## 3. SCOPE

The NAP policy applies to all departmental staff, operations, and records in all formats created and received as part of agency business that are not covered by the department's Records Authorities and the Administrative Functions Disposal Authority (AFDA) issued by the National Archives under section 24 (2) (b) of the *Archives Act 1983*, and are not needed as evidence of that business.

The policy recognises that records which need to be covered by a Records Authority are those required:

- For accountability purposes
- To support the ongoing efficient administration of the department's business which are linked to community expectations about records providing rights and entitlements, and the rights of staff
- To support department liability
- Because they are considered as having cultural or known historical value to the department.

Records that fall under these categories that are not covered in a current Records Authority must be retained until an authority is developed and approved by the National Archives. Their destruction under this policy is not permitted.

## 4. CONTEXT

The department supports a holistic approach to the management of all its information, including records, to improve efficiency, reduce administrative and operating costs, mitigate risks and increase accountability, and seeks to integrate its records management policies and procedures within a broader information management program. This NAP policy is an important component of the department's *Records Management Guidelines.*

The policy is supported by departmental procedures for some areas of activities, where the requirements to create, keep or destroy records is detailed. Any specific direction in a procedure to destroy certain records using NAP, or to retain records and capture them in the records management system (TRIM) must be adhered to. Records are managed according to destruction and retention requirements set out in the Department's Records Authorities, or in the Administrative Functions Disposal Authority, issued by the National Archives.

## 5. LEGISLATIVE FRAMEWORK

The department is committed to following the laws related to recordkeeping including

- the *Archives Act 1983*
- the *Privacy Act 1988*
- the *Freedom of Information Act 1982*
- the *Evidence Act 1995;* and
- the *Electronic Transaction Act* 1999.

The department also recognises its obligations to be openly accountable for actions under the *Public Service Act 1999*.

## 6. APPLICATION OF NAP

In addition to instructions set out in the departmental work procedures that direct the destruction of records using NAP, the following records may be destroyed as a normal administrative practice. Appendices A, B and C provide further guidance and examples of when/where NAP can be used.

***Facilities, transitory or short term items***

- appointment diaries, except Agency Head and SES level officers
- personal email
- listserv email, except those that relate to the business of the department, or might impact on the department's current or future deliberations on a matter relating to public policy (this type of email must be printed and placed on an appropriate departmental file)
- circulation copies of agency instructions, the internal staff newsletter (master copies must be printed and placed on an appropriate departmental file)
- unsolicited letters offering goods, services and conference attendance, where no action was taken to accept the offer
- information copies and duplicates of emails held in personal Outlook folders, personal drive, or section shared folders, that have been printed and placed on an appropriate departmental file
- information copies of final reports, policies, procedures internal and external correspondence and other documents kept on personal drives or in shared folders that have been printed and placed on an appropriate departmental file
- emails received that have been sent to multiple recipients, where the sender has responsibility for printing and placing the document on an appropriate departmental file
- emails capturing discussion where the final email has been printed and placed on an appropriate departmental file by the person responsible for the task
- unsolicited email (spam)
- computer backup tapes taken daily by the IT section can be destroyed after 7 days.

***Rough working papers and/or calculations***

These are usually incorporated into other files and are not needed as evidence of decisions to support the business of the department.

- routine or rough notes that have been produced as an aide memoire at meetings after their administrative use has passed
- meeting notes taken by a minute taker at internal departmental and interdepartmental meetings (destroy when minutes have been accepted)
- working papers and background notes used to support the preparation of correspondence, reports and departmental policies that are not needed to support decisions, actions or directives given in the documents.

***Drafts of departmental documents***

These are usually superseded by other work that is filed in an appropriate departmental file and are not needed as evidence of decisions to support the business of the department.

- all drafts of departmental documents (policies, reports, correspondence) containing corrections made to grammar and spelling
- drafts of whole-of-government policies and reports where no substantial change was made
- all drafts of internal departmental policies, procedures and reports that were not circulated for comment
- all drafts of routine correspondence where the answer is straightforward and fits into the department's policies and advice provided by the government, including ministerials, to members of the public seeking direction or guidance of departmental policies
- drafts that are not needed after the document has been finalised and filed.

***Copies of material retained for reference purposes only***

- copies of records made for reference purposes to support the development of reports, correspondence, policies and procedures
- material that someone else is responsible for filing.

***Published material which does not form an integral part of the department's record***

- duplicate promotional material and/or external publications (the area responsible for the publication must place one copy in the department's library and lodge one copy with the National Library of Australia according to legal deposit requirements).

## 7. RESPONSIBILITIES

***The Deputy Secretary (Governance)***

- authorise the NAP policy
- promote compliance with the NAP policy.

***The Manager, Records Management Unit***

- monitor and review the NAP policy
- ensure that the department's NAP practices comply with the National Archives guidelines
- develop strategies to support the NAP policy including:
    - develop specific guidelines
    - address induction sessions for new staff
    - place the policy and guidelines on the intranet
- incorporate NAP policy directives into agency work procedures
- incorporate NAP policy directives into the design and development of the department's records management systems, including IT systems.

***All managers and supervisors***

- promote an understanding and use of the department's NAP policy to staff under their supervision.

***All departmental employees***

- understand their responsibilities that relate to the use of the department's NAP policy

- follow directions in this policy and any work procedures about using NAP to destroy records
- ensure that the records they destroy are not agreements or legal documents
- ensure that the records they destroy using NAP are not needed to:
    - clarify, support or give context to an existing record
    - show how the agency business was carried out
    - show how a decision was made
    - show when or where an event happened
    - show who made a decision or gave the advise
    - protect the right or obligations of government or private individuals; or
    - support legal proceedings.
- if uncertain of responsibilities or whether the record can be destroyed using NAP, seek guidance before destroying any record from the Records Management Unit.

## 8. MONITORING

Monitoring of the policy should be carried out by the Records Management Unit, supervisors and managers.

## 9. REVIEW

The Records Management Unit will review the NAP policy every 3 years or earlier if required.

## 10. AUTHORISATION

This NAP policy has been approved by:

Renee Leon

Deputy Secretary - Governance

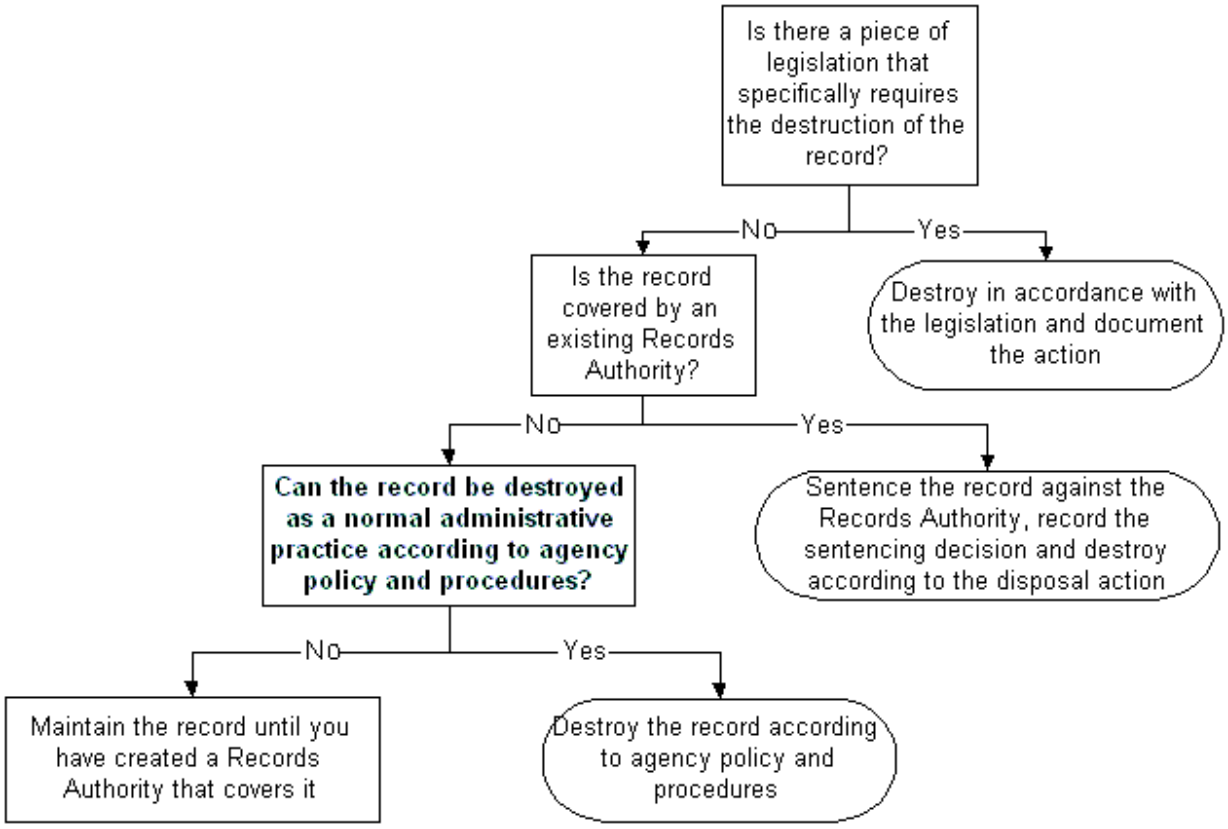
Department of the Prime Minister and Cabinet

August 2013

Appendices:

A. NAP flowchart
B. NAP checklist
C. List of material that can be destroyed under the NAP – examples and exceptions

## 11. APPENDIX A - NAP FLOWCHART




**This flowchart illustrates the process of deciding when you can destroy a record using a NAP (www.naa.gov.au)**

## 12. APPENDIX B - NAP CHECKLIST

Any decision to destroy a record as NAP should be made after considering the context of the business activity that it supports. With this in mind, ask yourself the following questions about the record:

Is the record covered by a specific law or a Records Authority issued by the National Archives?

If not, is the record:

- needed to clarify, support or give context to an existing record?
- needed to show how the agency business was carried out?
- needed to show how a decision was made?
- needed to show when or where an event happened?
- needed because it indicates who made the decision or gave the advice?
- needed because it contains information on the rights or obligations of government or private individuals?
- a formal draft of a Cabinet submission?
- a draft of an agreement or legal document?
- likely to form part of a record that will be needed to support legal proceedings?

If the answer to all these questions is no, then you can consider destroying the record as a normal administrative practice. If the answer to any question is yes, the record should be retained so that appropriate coverage under a Records Authority can be developed.

## 13. APPENDIX C - LIST OF MATERIAL THAT CAN BE DESTROYED UNDER THE NAP – EXAMPLES AND EXCEPTIONS

| Types of NAP Record | PM&C Samples and exceptions |
|---|---|
| • An email that is a duplication | You might find an email thread that is more recent than an email already filed. You are allowed to replace the older version as long as the new thread incorporates all the emails in the thread. |
| • Unimportant telephone messages | Telephone numbers, return calls etc. |
| • Copies of superseded manuals or Instructions | Where Corporate Executive Instructions (CEIs) or manuals are out of date and have been superseded. However, a master set showing old versions and the changes made for the current version, including any or all of its parts must be kept. |
| • Catalogues and trade journals | Any extracts of information taken from published journals and publications may be destroyed or kept for reference. Please note: Material on loan from the library are PM&C's assets, and must be returned to the library. |
| • Division/Branch/Team copies of material used for easy reference | Copies of invoices, payment details, reports, where originals have been retained on official files may be destroyed.<br><br>Copies of accounts and purchase orders may be destroyed. The Finance and Resource Services Section is responsible for keeping the original accounting documentation in accordance with the AFDA. |
| • Rough drafts of reports, correspondence, routine or rough calculations | This refers to minor and inconsequential material and duplicates. Submitted drafts that show major changes to the direction and development of a record should be kept. |

| | |
|---|---|
| • Address lists | If the address lists do not form part of a Business System, these lists may be destroyed when action has been completed or reference ceased. |
| • Information copies of press cuttings, press statements or publicity material | Copies may be destroyed. Original and significant press statements are to be placed on the file. Marketing material developed in PM&C is also a record and is to be kept on official files. |
| • Requests for copies of maps, plans, charts etc. | If the map, plan or chart forms part of the record, then it should be kept. The request to obtain these items may be destroyed. |
| • Calendars, office diaries and appointment books | Calendars and/or diaries that show important decisions or instructions to staff on major projects should be kept. Routine or insignificant calendar or diary entries may be destroyed.<br>Exception: Secretary and SES diaries must be kept. |
| • Routine statistical and progress reports, compiled and duplicated in other reports | If any of this material is used as reference, or referred to in a report then you should retain the copy on a file. Otherwise they may be destroyed. |
| • Duplication of TRIM files | If a file is created in error, it must be returned to the RMU. The RMU will update the TRIM database to reflect action taken and ensure that the file is destroyed under the correct authority. |

Australian Government
Department of the Prime Minister and Cabinet

# KNOWLEDGE AND INFORMATION MANAGEMENT (KIM) STRATEGY

The Corporate Plan 2016-20 defines the Department's purposes, how to measure performance against them, and the key areas of coordination. The Department is required to provide well-founded, clear and persuasive advice and develop national policy on signature issues of central importance to the Government and the Prime Minister. This Strategy outlines high-level approaches to organising, sharing and using the Department's knowledge and information (coordination and collaboration). It details behaviours and activities so information can be found, stored and accessed both efficiently and securely. As a knowledge-based organisation, the Strategy aids the sharing of knowledge and expertise amongst the Department's stakeholders to encourage innovation.

The KIM Strategy is an outcome of the ICT Strategy. It aligns with the People Strategy, the Corporate Blueprint and the Department's Strategic Statement since there is a focus on guiding behaviours, improving capabilities and supporting core strategic priorities. This strategy will also be delivered in accordance with the Information Management Policy.

## STRATEGIC GOALS

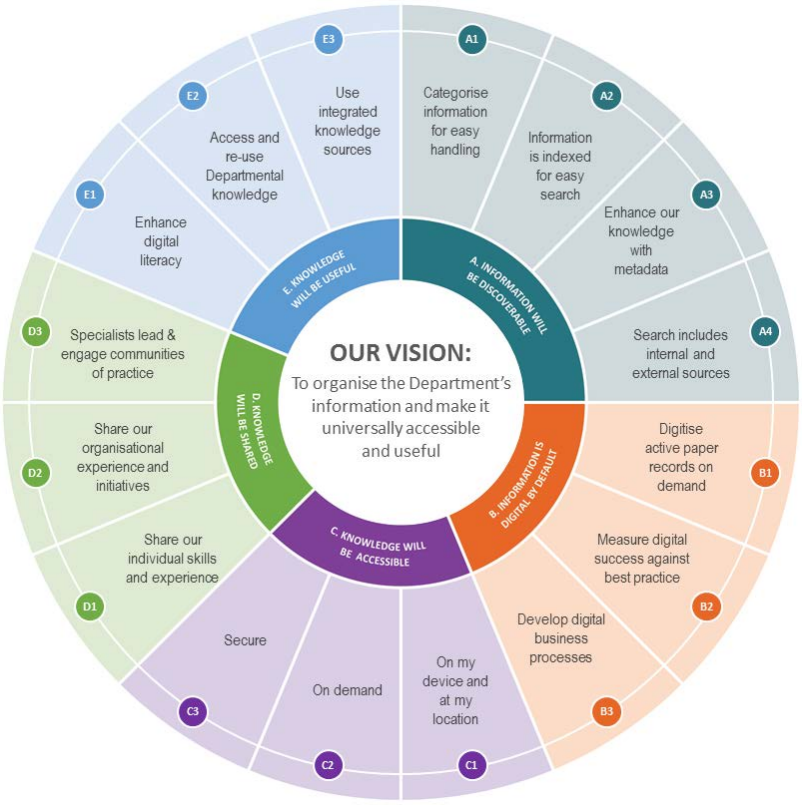
### A. Information will be discoverable
Information can be found and described using common sense terms which make good sense to the user.

### B. Information is digital by default
Information will be available on a secure electronic platform in a digital form where appropriate.

### C. Knowledge will be accessible
Information can be securely accessed at any place or time with appropriate controls.

### D. Knowledge will be shared
Our people (through processes and systems) are encouraged to share and exchange their experience, know-how and information.

### E. Knowledge will be useful
Our advice and our people will leverage what we know and are able to source through active and integrated knowledge exchange mechanisms.




## DRIVERS FOR CHANGE
The KIM Strategy is driven by the need to:

- Ensure our people have information at their fingertips for developing advice
- Ensure our information is secure yet accessible
- Categorise information to increase utility and improve discoverability
- Ensure our information is easy to retrieve
- Ensure the information architecture is designed for simplicity
- Move to a 'paper-lite' environment
- Be an exemplar for Digital Continuity 2020

## GOVERNANCE
Progress of the KIM Strategy will be monitored by, and reported to, the Executive Leadership Group through the Operations Committee

***Knowledge is:***
*Information with full context (a mix of experience, principles, additional information, expert insight and proven intuition). It is closely linked to doing, and suggests that know-how and understanding has been used to create it.*

***Information is:***
*Categorised and condensed data that has relevance and purpose. It answers questions beginning with who, what, where, when, and how many. It may show a trend or perhaps indicate a pattern for a given period of time.*

## MEASURING SUCCESS
Success will be measured by:

- Feedback on the relevance of search results
- Count of paper-based sources migrated
- Reduced cost of knowledge and information processes
- Positive feedback in staff surveys

## WHAT'S IN IT FOR ME?

- Improved search tools
- Information that produces higher quality, more relevant search results
- Encouragement to share and develop ideas with colleagues
- Ability to access and search corporate knowledge including access to subject matter experts

Australian Government
Department of the Prime Minister and Cabinet

# Retention and Destruction of Original Records

## BACKGROUND

### Digital Transition Policy

As of 1 January 2016, the Department reduced the creation of paper files to meet the requirements of the whole-of-government Digital Transition Policy. This policy aims to move government agencies to digital recordkeeping practices for efficiency purposes. This means that the majority of our records will be created, stored and managed digitally and where possible, paper records will be scanned reducing the need for new paper files to be created.

There are certain exceptions to this rule which means that some records cannot be reproduced and/or stored digitally. This document is intended as a quick reference guide for business areas within the Department about which records must be retained in hard copy and which records may be destroyed after digitisation / scanning and saved into either ShareHub, PDMS or HP Records Manager.

### When should original records be retained?

#### Records subject to a Records Disposal Freeze or Retention Notice

There a number of records disposal freezes and retention notices that the National Archives of Australia has issued relating to controversial issues or events, or judicial proceedings. Generally, these state that agencies must not destroy any relevant records.

If an original record relates to anything covered within a certain disposal freeze or retention notice, you must ensure that you are permitted to reproduce and dispose of the record under the terms of the freeze or notice before taking any action. Current freezes and notices that affect PM&C records can be found here.

#### Records likely to be required as evidence for a current or future judicial proceeding

If you believe an original record (digital or physical) may be required as evidence in a future judicial proceeding, including where regulatory action is current being undertaken which may lead to a judicial proceeding, you must not destroy the record unless a risk assessment is undertaken. When conducting this risk assessment, you should consider:

- The likelihood of future proceedings being commenced;
- The likelihood of the original records being required as evidence if proceedings are commenced;
- PM&C's overall business
- A cost/benefit analysis to retain or destroy the original record
- The public perception that may arise from the destruction of the original record; and

- Whether any current or future copying, or migration of the original record will impact the admissibility of the record as evidence in judicial proceedings.

When the judicial proceedings are finalised or it is no longer considered that proceedings will be commenced, you may destroy the records provided they have been successfully reproduced digitally and stored into ShareHub or HP Records Manager.

**Please note: You must consider whether the original format of the relevant document is necessary to the proceedings, not simply the content.**

### Records likely to be subject to a current application for access under the *Freedom of Information (FOI) Act 1982, Archives Act 1983* or other legislation

When the original record (digital or physical) is likely to be subject to a current FOI, Archives Act or other access request, you must not destroy the original record.

**Please note: This does not apply to records that will potentially be subject to an FOI, only to records that are potentially subject to a current FOI**

## Original records that must be retained in a physical format within PM&C

### Classified records

Any records classified as CONFIDENTIAL, SECRET and TOP SECRET must be retained in hard-copy form and stored on a Departmental file. There are currently no electronic recordkeeping systems available in the higher network.

### Records required to be retained for other business purposes

Some original records may need to be retained in hard-copy format where a strong case can be made that they are necessary for other business purposes such as:

- Large volumes of paper records that have been received from external sources; or
- Legacy paper filing that is not practical to be digitised.
- Where original paper records cannot be successfully reproduced or stored electronically for technological reasons;
- Where electronic reproduction or storage cannot be relied upon for authenticity, accuracy or useability; or
- Where a business practice relies heavily on a paper-based workflow

### Records with Intrinsic qualities

Certain records may have *intrinsic value*. Intrinsic value is not related to the record's information value, but comes from the particular characteristics that the record has in its original format, which would not be carried over, and therefore lost, in a digital reproduction of that record. In most cases a record's intrinsic value is judged by considering PM&C's history and heritage. These characteristics can be either *physical* or *intellectual*.

**NB:** The concept of intrinsic value can be subjective, and the relevant business area is responsible for determining if a record has intrinsic value or not. The Records and Information Management Team is always available to assist with such a determination.

### Records with Physical Intrinsic qualities

- Questionable authenticity, date, author, or other characteristic that is significant and ascertainable by physical examination, or where controversy around the subject may warrant the original to be retained for later forensic proof (for example: Land Title Deeds and Signed Program Funding Agreements for Land / Infrastructure / Housing Capital Expenditure).
- Records on rare or obsolete formats including particular types of paper, vellum, objects, volumes with unique form or binding, magnetic storage devices, punch cards, wax cylinders, glass negatives gramophone discs, etc.
- Rare or original objects such as mint issue stamps or coins, rare books or seals where monetary value may be a factor.
- Physical features, such as wax seals, watermarks, cross-written correspondence or scrapbooks with rare and unique content.
- Records where the original medium conveys meaning such as overlay drawings. This includes records where the information cannot be accurately reflected in digital format.
- Records of artistic or cultural significance, or with aesthetic quality such as art, cultural artefacts, photographs, architectural drawings, illuminated manuscripts, copyright exhibits, design drawings.
- Value for use in exhibits, where the record itself imparts a sense of historical significance or of the significance of a person or event to which it relates.

### Records with Intellectual intrinsic qualities

- Original documents of general and substantial public interest due to a direct association with famous or historically significant people, places, things, issues, or events such as the Prime Minister or Governor-General, the Constitution or treaties. Includes final speeches by the Prime Minister and Governor-General and speech notes.
- Primary establishment documents with significance to the establishment or continuing legal basis of an agency or institution, the functions or powers of government, or the formulation of the highest levels of legislation.
- Policy documents with significance to the formulation of the highest levels of policy within Government. Includes major policy documentation signed by the Prime Minister and signed COAG joint ventures.
- Significance or value to individuals as an artefact or evidence of their ancestry or heritage which contain original photographs, handwriting etc.

To meet this inclusion, the record must also be identified as 'Retain as National Archives' (RNA) or Retain Permanently (RP) under the Department's Record's Authority. If these requirements are met, then a business case will need to be sent to the Records and Information Management Team, and a paper file will be created to store this information. For further guidance, please contact the Records and Information Management Team x5599 or help-recordsmanagement@pmc.gov.au.

## Original records that can be destroyed by PM&C staff following digitisation

The National Archives of Australia (NAA) has issued a General Records Authority (GRA 31) which provides authority for the Department to destroy certain source records that have been copied. This is endorsed for use by the Department by the Records and Information Management Team.

This authority covers all agency records created on or after 1 January 1980. This authority authorises the destruction of original records which the Department 'owns' or for which it is responsible, subject to certain conditions and exclusions if:

- They have been successfully reproduced digitally and stored as a Departmental record; and
- No specified exclusions apply.

Any original records (digital or physical) that do not fall under any of the categories listed above may be destroyed following digital reproduction and storage in ShareHub or HP Records Manager.

The *Evidence Act 1995* allows the admission as evidence of copies of records where they copy has the necessary degree of authenticity, reliability and useability. This means that as long as you have met these requirements, you may destroy the original signed copy of the contract.

The following are examples of original documents that may be destroyed following successful digital reproduction and storage (where no other exclusions listed above apply):

- Signed briefs from the PMO in PDMS
- Credit card receipts and travel documents
- Tender documentation
- Authorisations
- Signed Departmental contracts
- Forms
- Copies of documents that are provided for reference

Successful reproduction must be functionally equivalent to the original record for business and legal purposes. This reproduction must ensure that the record is authentic, accurate and is a reliable copy able to be used for the same business and legal purposes as the original record would be used. The record must also be managed as a record within ShareHub or HP Records Manager.

All scanned documents must be legible and any features such as colour are present in the scanned document.

For more information, please contact the Records and Information Management Team x5599 or help-recordsmanagement@pmc.gov.au.