Australian Government
Australian Public Service Commission

Information and Records Management SHD20-22426

Intranet Page

What is a Record?

All information created, sent and received in the course of carrying out your job at the Australian Public Service Commission is potentially a Commonwealth record. Determining if something is a record or not depends on the information and the context – basically, if it is related to the business of the APSC then it is a record.

For example, an email to your manager briefing them on a topical issue is a record, whereas an email to the same person letting them know their car window has been left open is not a record.

Records come in digital, paper and other formats, includingemail, website pages, SMS messages, information in business systems, databases, datasets, letters, faxes, maps and plans, as well as images in photographs, film, video and DVD. Depending on what business is being carried out, records can also be objects such as samples and exhibits.

As government business is increasingly conducted digitally, records such as email and records of web transactions have become central to our daily work.

Why do records matter?

Records are an essential part of an accountable and transparent government. The APSC recognises information is a corporate asset. Records provide evidence, justify decisions and demonstrate the process followed. The creation, maintenance and accessibility of Commonwealth records are key elements of sound public administration and accountability.

Legislation

The importance of good record keeping to accountable and transparent government, is emphasised by legislation such as the Freedom of Information Act 1982 and the Archives Act 1983 (which provide for public access to government information) and other key legislation such as the Public Governance, Performance and Accountability Act 2013, the Public Service Act 1999 and the Evidence Act 1995. There are legislation that includes information and records management requirements, see Appendix A.

The APSC is also committed to the principles and practices set out in whole-of-government sources (including legislation, policies, standards and advice) and best-practice standards of information and records management.

These best practice standards are influenced by the principles from the Australian Government Digital Continuity 2020 Policy, Secure Cloud Strategy Policy, Protective Security Policy Framework and the Cyber Security Strategy.

Codes of conduct

Public sector values and code of conduct are outlined in sections 10, 10A and 13 of the Public Service Act 1999. The APS Values and Code of Conduct provide that all Australian Government employees need to be accountable for their actions. Records support accountability.

Efficiency and corporate memory

Records ensure that information is available over time. By building corporate memory, records ensure agencies can carry out their business efficiently and effectively.

Protection of rights and entitlements

Records provide evidence of decisions about the rights and entitlements of individuals and companies. With adequate records, the government can explain its actions and decisions and maintain transparency with consistent decision making.

Why do records matter to you?

In your everyday work, making and keeping records helps to:

- find and use the information you need
- share information with colleagues
- reuse good work done in the past
- produce evidence when required to explain a decision.

Records can also help protect you and the APSC when something goes wrong or a decision or action is challenged. In the longer term, creating and keeping records helps future generations understand Australia's history, society, culture and people. The most valuable government records will be kept permanently in the National Archives as part of Australia's heritage.

What are your records management responsibilities?

All staff have a responsibility to appropriately capture, store and access records associated with their work. This includes:

- **Always** keeping appropriate records
- Ensuring records are held in Sharehub or the relevant EDRMS
- Using appropriate and meaningful titling conventions
- Store and handle records according to APSC's policies and procedures.
- Only destroy, delete, alter or remove records following appropriate authorisation

- Take care with records to prevent them from being lost or damaged
- Check protective markings on records and ensure they are managed appropriately
- Supervisors and managers should ensure staff have training and ongoing support to manage their records effectively.

How should you name or title records?

Giving records meaningful titles will point you and others to the information in the future, saving time and effort.

Make sure the titles:

- Are meaningful and easy to understand
- Avoid vague terms like 'miscellaneous'
- Distinguish between similar records
- Spell out abbreviations and acronyms.

Your APSC group or team may have specific guidelines for you to follow, such as a file plan or naming conventions.

The ShareHub Titling Conventions document will assist Teams / Groups to develop a consistent naming approach. An important note the maximum length of characters that can be included in a ShareHub title/file path (URL) is 256 characters.

Where should you keep records?

All official records of the agency should be retained in Sharehub which is the APSC approved Electronic Document Records Management System (EDRMS), or in an appropriate business information system, e.g. APSED. Records classified up to PROTECTED classification should be stored in ShareHub. Records that are classified beyond the PROTECTED classification security should not be captured or created in ShareHub and stored appropriately in the nominated system

OFFICIAL records (regardless of format) stored in shared drives, personal drives, personal email folders, the Cloud, local applications, cabinets, workstations and on backup drives are not compliant with APSC's information and record management obligations.

The Parliamentary Workflow System (PWS) is a whole of government system called Parliamentary Document Management System (PDMS+). Documents that are managed within PDMS+ include Ministerial briefings, Question Time Briefs, Ministerial Correspondence and Questions on Notice, following Senate Estimate and Committee Hearings. Documents managed within PDMS+ are not required to be saved in ShareHub as this is an approved EDRMS. Some Groups choose to save draft versions or templates of PDMS briefings in Sharehub for easy reference and access.

Can you delete or destroy records?

The destruction of records is governed by the Archives Act and other legislation.

Before you make decisions to delete or destroy records you must:

- find out which records you are responsible for keeping
- find out which records you can delete or destroy (some low-value records can be routinely destroyed after they no longer have business use)
- always follow authorised procedures
- ask your supervisor or records manager if unsure.

Under the Archives Act 1983 and the Crimes Act 1914, APSC records cannot be disposed of other than in accordance with the approved NAA disposal authorities. The disposal authorities relevant to the APSC are:

- the Administrative Functions Disposal Authority AFDA Express Version 2 and
- the Australian Public Service Commission Records Authority.

Please note that lists of destroyed APSC official information and records should be retained as national archives.

Records created and received as part of APSC's business that are of ephemeral value and are not covered under a Records Authority can be considered for destruction using NAA's Normal Administrative Practice (NAP) provisions. These records can be disposed of by the creator, using the appropriate method, without seeking formal approval

How should you manage email?

It can be difficult to manage business related email due to the volume and speed at which they are created and received.

Some tips for managing email records include:

- Understand which email you are responsible for capturing.
- Emails that contain decisions should always be saved in ShareHub.
- Capture email in ShareHub where they can be accessed and shared.
- Emails kept in personal or team Inbox, are not compliant with APSC’s legislative obligations.
- Email titles need to be meaningful. Sometimes the 'subject' line of an email is not descriptive enough.
- Email that does not relate to business, such as personal messages or ones that are received for information only, do not need to be kept.

When do you need to restrict access to records?

The need-to-know principle applies to accessing all corporate records and information to guard against the risk of unauthorised access or misuse of information, i.e. the availability of official information should be limited to those

employees who need to use or access the information to do their work e.g. to authorise a document to be finalised.

Information and records should be accessible within the APSC, unless they relate to:

- national security
- privacy of individuals and organisations
- legally or commercially sensitive information

Records that need to be protected for these reasons must be given a classification rating and captured in an appropriate secure location or system. From time to time, you may need to review when, and by whom certain actions were taken on a document. You can use the ShareHub Activity Log to see a chronological list of actions performed on the document, and who performed them.

APSC staff are responsible for assessing the security requirements for the information and records they handle and applying the appropriate security levels to information and records. The originator must determine whether information and records being generated is OFFICIAL information/record (intended for use as an OFFICIAL record) and whether that information/record is sensitive or security classified. In the majority of cases, APSC information and records will be OFFICIAL in nature.

For more information about security classification and protecting records, contact APSC Information and Records Management Manager or APSC IT Security Adviser. There are also details available here following the changes to information classifications in 2019.

Can you provide information to the public?

There is a legal and regulatory framework that governs the general disclosure and use of official information by APS employees and access by the public. Apart from the Public Service Act 1999 (including the Code of Conduct), the framework includes:

- Archives Act 1983
- Crimes Act 1914
- Criminal Code Act 1995
- Freedom of Information Act 1982
- Privacy Act 1988

In providing public access to government information you must follow APSC procedures and business processes. Refer requests to the appropriate person or area within your agency.

Requests for information must be treated consistent with the requirements of the FOI Act and parliamentary questions answered in accordance with the relevant sections of Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters - February 2015.

Information can be disclosed except in the course of duties might:

- damage Australia's relations with foreign States or
- damage the Commonwealth's relations with the States or
- prejudice the conduct of a prosecution or civil litigation to which the Commonwealth or the APSC is party or
- prejudice a tender process or
- prejudice a certified agreement negotiation being conducted by the Commonwealth or an agency or
- damage an individual.

For more information, please consult the APSC Information and Records Management Policy and Procedure or contact the APSC Information and Records Management Manager.

Appendix A

Legislation that includes information and records management requirements

- Archives Act 1983
- Archives Regulations 2018
- Australian Public Service Commissioner's Directions 2016
- Commonwealth Procurement Rules (CPRs)
- Crimes Act 1914
- Criminal Code Act 1995
- Electronic Transactions Act 1999
- Electronic Transactions Regulations 2000
- Evidence Act 1995
- Freedom of Information Act 1982
- Freedom of Information (Charges) Regulations 2019
- Freedom of Information (Disclosure Log – Exempt Documents) Determination 2018
- Legally binding privacy guidelines and rules
- Fair Work Act 2009
- Fair Work Regulations 2009
- Privacy Act 1988
- Privacy Regulation 2013
- Public Governance, Performance and Accountability Act 2013
- Public Service Act 1999
- Public Service Regulations 1999
- Senate Continuing Order for the production of departmental and agency file lists (Harradine Motion)

The APSC is also committed to ensuring that its records management and business systems comply with established standards and major reports into recordkeeping in the Commonwealth such as:

- Australian Government Information Security Manual
- Australian Government Secure Cloud Strategy
- Australian Standard for Records Management - AS ISO 15489 – 2016
- Australian Standard for Managing Records in an Electronic Environment – ISO 16175
- Australian Government Recordkeeping Metadata Standard
- Cyber Security Strategy
- Digital Service Standard
- Digital Continuity 2020 Policy
- Protective Security Policy Framework.

Sharehub Record ID SHD20-22426