Group Records Management Policy

Policy Level:	1
Accountable Executive:	Group Chief Financial Officer and Executive General Manager, Finance and Commercial Services
Date Approved:	21 August 2019
Date Effective:	21 August 2019

auspost.com.au

Contents

Statement of Policy

Overview

Reliable and useable Records support the Group by providing evidence of decisions and activities, whilst also contributing to our overall business efficiency and efficacy.

This Policy sets out a consistent approach towards the management of Records across the Group. This Policy supersedes all previous record management policies.

Rationale & Scope

The purpose of this Policy is to set out a framework for the creation, maintenance, storage and disposal of Records within the Group.

This Policy applies to all information handled by the Group, regardless of format, and regardless of how it is created, distributed or stored (for example, whether it is typed, handwritten, printed, filmed or computer-generated).

Audience

All Workforce Participants remain subject to obligations and principles identified through this Policy.

Application

The Group is committed to implementing best record management practices and systems. This Policy requires:

- Adherence by all Workforce Participants and contracts to the Policy Principles;
- Management accountability through Accountable Executive Policy ownership and Executive Team
- adherence through their respective business units;
- Strong use of Enterprise technology, people and processes;
- Policy compliance monitoring (including reporting of failures to comply); and
- Periodic audit of adherence to the Policy in line with Internal Audit guidelines.

Policy Principles

We expect our Workforce Participants to adhere to the following Policy requirements:

- Records must be captured in approved APG record management systems and capable of registering content, structure and context of the Record.
- Records must be retained for as long as operationally and legally required under applicable Records Authorities, or other stipulated retention periods.
- Records must be destroyed when they reach the end of their required retention period (including as set out in applicable Records Authorities).
- Records of short-term value that are not covered under a Records Authority or retention period, may be destroyed in the normal course of business under Normal Administrative Process (NAP).
- Records should be protected and secured to maintain its integrity and authenticity in line with our Privacy Policy and Information Security Standards.
- Workforce Participants are responsible for the transfer of Records to designated storage facilities, in line with approved Transfer processes.
- Records must be able to be recoverable from any system or storage location which retains them.

- Records must remain available in a useable format, regardless of any technology changes and/or Records migration which may occur.
- The disposal of Records must be:
    - Irreversible so that there is no reasonable risk of the information being recovered again.
    - Undertaken securely and with the same level of security that was maintained during the life of the Record.
    - Be documented as proof of destruction may be required in legal proceedings.

Awareness, Training & Induction

Here are some of the things we will do to keep this Policy top of mind:

- This policy will be available on the intranet and to subsidiaries and associated entities.
- We will provide training about your rights and responsibilities.
- Regular reminder about your responsibilities under the Policy will occur.

Where applicable the Policy will be implemented through Standards. These standards require regular review and updates to maintain currency with internal and external requirements.

Enforcement & Monitoring

Business unit management have accountability to enforce this Policy and deal with intentional non-compliance through both the performance management and disciplinary process. APG will conduct reviews to ensure ongoing compliance with this policy and supporting standards. These reviews will be undertaken regularly by Group Risk and/or Group Compliance.

Breaches, Variations & Exemptions

All potential Policy breaches will be investigated. In support of this Policy, we will follow a formal process for those who breach this Policy.

All breaches of this Policy must be escalated to Group Compliance, who in turn will escalate to the Enterprise Risk Council or the Board Audit & Risk Committee if appropriate. Management may seek variation to Policy requirements by seeking specific written approval from the General Manager, Group Compliance.

Any proposed exemptions should be submitted to the Policy Content Owner and Policy Administrator for review and possible endorsement, with final approval granted by the Policy Owner.

Reporting

An Enterprise summary outlining any contraventions of Policy requirements will be reported to business unit executive leadership at least quarterly through existing Group Compliance dashboards.

Review

This policy will be reviewed by the Accountable Executive at least every three years and amended as deemed necessary (based on changes to strategy, government policy etc.).

Policy Guidelines

Ownership of Records

All Records (regardless of format) created, sent or received by Workforce Participants in the course of their duties on behalf of the Group, remain the property of the Group and subject to its overall control. The only exception is if there is in place a contract or a legally binding agreement that states otherwise.

Destruction of Records and NAP

Under the *Archives Act 1983* (Cth), it is an offence to destroy any Commonwealth record without authorisation from the National Archives of Australia (NAA). As Australia Post is a Government Business Enterprise (GBE), any record that is the property of Australia Post is deemed to be a Commonwealth record.

The NAA permits some records that are not covered under a Records Authority to be destroyed in the normal course of business without seeking formal authorisation under NAP.

Examples of such records include:

- Working papers, notes and calculations used in the preparation of other records
- Drafts, superseded versions of documents
- Multiple and reference copies of documents
- Published material (unless you published it)
- Electronic copies of documents where hard copy has been printed and filed
- Stationery and forms
- Old manuals

Records may be destroyed when they reach the end of their required retention period set out in Records Authority issued by the NAA, or other stipulated retention period for Group subsidiaries.

Authorised record management systems

Records subject to current retention authorities should be captured in the Group's existing Authorised Recordkeeping System - TRIM. TRIM allows the user to assign registration numbers to Records allowing tracking and is compliant with the Australian Standard for Records Management AS ISO 15489.

Any Group system that captures records must be capable of managing the following processes:

- can collect all information required for the activity – it must be fit for purpose
- be capable of capturing content, structure and context of the record
- provide protection of record integrity and authenticity
- be readily accessible to all Workforce Participants who need to use the records contained within the system
- ensure the recoverability of records in the event of a disaster
- ensure the availability of records in a usable format through technology changes and migration.

Roles & Responsibilities

Policy Governance

Requirement	Responsible area/Role	Activities
The Enterprise Risk Council (ERC) must report on to the implementation of governance frameworks and policies to the Audit Risk Committee (ARC) and Board	ARC and Board	The ARC will ensure appropriate governance mechanisms and control frameworks are in place.
Responsibility for the Policy.	Accountable Executive	To oversee the application of the Policy and procedures supporting it.

Policy Operation

Requirement	Responsible area/Role	Activities
Identifying and managing risks associated with their business objectives, strategic activities and operations.	Managers	Fostering an environment that makes records management a responsibility for all employees, articulating clear standards and procedures to encourage application of the Policy and monitoring and enforcing compliance with the Policy as required.
Comply with recordkeeping obligations, policies and procedures. Undertake relevant training.	Employees	Complying with recordkeeping obligations, policies and procedures relevant to their work responsibilities.

Policy Monitoring & Oversight

Requirement	Responsible area/Role	Activities
Periodic review to test policy implementation and accountable executives process for testing/validating compliance to this policy	Group Compliance	Option to undertake periodic reviews to test policy implementation as per the policy cover sheet and Accountable Executive process for testing/validating compliance to this policy and reporting Breaches and incidents.
Periodic internal audit for compliance to the policy	Internal Audit	Option to undertake internal audits to determine level of compliance with the Policy, and ensure Breaches and Incidents are realised and reported appropriately

Glossary

Term	Definition
APG	The Australia Post Group ('Group', 'we' or 'us'), comprising of the Australian Postal Corporation and all its owned or controlled Australian entities and businesses, including StarTrack, SecurePay, POLi Payments and Decipha. is legally required to maintain proper records of its business activities and decision-making.
Business Activities	Any duties conducted for the Group including advice, decisions, actions, events, meetings, conversations, correspondence or other activities.
Commonwealth Record	A 'Commonwealth record' is 'a record that is the property of an authority of the Commonwealth but does not include a record that is exempt material'.
GBE	Australian Commonwealth government business enterprise
NAA	National Archives of Australia
Policy	This Group Records Management Policy
Record	Information that is created, received or maintained in the course of carrying out business activities which supports Australia Post's fiscal, legal and business transactions or functions. They provide proof of what happened, when it happened and who made decisions can be in any format – paper or electronic, e.g. photo, plans, sound recordings, databases, microforms etc. Examples of records include: • electronic documents • hardcopy documents • emails • videos • data in business systems • web content • social media • maps, models, plans, drawings and photographs.
Records Authorities	**Australia Post Records Authority (APRA)** This Authority is based on the identification and analysis of the business of Australia Post. It takes into account the agency's legal and organisational records management requirements, and the interests of stakeholders, the agency and the National Archives of Australia. This Authority gives Australia Post permission, under the Archives Act 1983, for the destruction, retention or transfer to the National Archives of Australia of the records described. The Authority sets out those records that need to be retained as national archives and the minimum length of time that temporary records need to be kept. Retention periods for these temporary records are based on: an assessment of business needs; broader organisational accountability requirements; and community expectations; and are approved by the National Archives of Australia on the basis of the information provided by the agency.

Term	Definition
	Administrative Functions Disposal Authority (AFDA) The Administrative Functions Disposal Authority (AFDA) identifies minimum retention periods for Commonwealth records. This Authority covers the records relating to the administrative functions performed by the Commonwealth and its agencies. It applies to central or national offices, State/Territory or branch offices, local offices and overseas posts. It applies to all records created since Federation, regardless of format.
Workforce Participants	Anyone who performs work for the Australia Post Group, or on our behalf, including: • employees (permanent, fixed term or casual) of any company in the Australia Post Group; • contractors, consultants, licensees and agents, as well as their employees and • subcontractors; • interns, work experience students, and volunteers; and • any other third parties performing services for or on behalf of the Australia Post Group

Policy Administration

Key Policy Information

Administrative Area	Policy Information
Document Title	Group Records Management Policy
Policy Level	1
Version No	1

Policy Owners and Governance Forums

Administrative Area	Owner / Forum
Accountable Executive	Group Chief Financial Officer and Executive General Manager, Finance and Commercial Services
Policy Owner	Chief Risk Officer
Policy Administrator	General Manager, Compliance
Policy Content Owner	General Manager, Compliance
Review and Approval Body	Audit Risk Committee (Endorse) Australia Post Board (Approve)

Key Dates

Administrative Area	Date
Policy Approval Date	21 August 2019
Policy Effective Date	21 August 2019
Next scheduled review	August 2022