National disabilityinsurance Agency

Records Management Policy

Release:	30 August 2013
Date:	30 August 2013
Author:	Enabling Services
Owner:	Records Management
Client:	All NDIA employees and contractors
Document Number:	26909313v3

Revision History

Date of next revision:

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
30 Aug 2013		Original Draft	
26 Sept 2013	30 Aug 2013	Updated draft	No
10 Feb 2014	26 Sept 2013	Final draft	No
21 May 2014		Replaced CAC Act with the PGPA Act	No

Approvals

This document requires the following approvals. A signed copy should be placed in the policy file.

Name	Signature	Title	Date of Issue	Version
s22(1)(a)(ii) - irrelevant material		Branch Manager – Property Division	10 Feb 2014	1
s22(1)(a)(ii) - irrelevant material	*Approved 14 Feb 2014*	Chief Executive Officer	12 Feb 2014	2
s22(1)(a)(ii) - irrelevant material		Chief Information Officer		3

Distribution

This document has been distributed to:

Name	Title	Date of Issue	Version

National disabilityinsurance Agency

Overview

Purpose

The purpose of this policy is to establish a framework for the creation and management of records within the organisation. NDIA is committed to establishing and maintaining recordkeeping practices that meet its business needs, accountability requirements and stakeholder expectations.

Principles

NDIA's Recordkeeping Policy exists in the context of the following principles, which are designed to promote best practice in recordkeeping:

Accurate: records will correctly reflect what was communicated, decided or done.

Adequate: records will be adequate for the purposes for which they are kept.

Audited: recordkeeping systems, procedures and practices will be audited to ensure compliance with regulatory requirements.

Authentic: records will be what they purport to be.

Complete: a record will contain not only the content, but also the structural and contextual information necessary to document a transaction. It should be possible to understand a record in the context of the organisational processes that produced it and of other, linked records.

Compliant: recordkeeping and management of those records will comply with legal and administrative requirements.

Comprehensive: records will document the whole of the business of the organisation.

Inviolate: records will be securely maintained to prevent unauthorised access, destruction, alteration or removal.

Made: records will be made automatically by business systems or intentionally by staff, to document and facilitate the conduct of business.

Reliable: recordkeeping systems, procedures and practices will work reliably to ensure that records are credible and authoritative.

Retained: records will be retained for as long as they are needed.

Routine: recordkeeping systems will be used when transacting business.

Systematic: records will be made, maintained and managed systematically.

Useable: records will be identifiable, retrievable, accessible and available when needed.

1. Introduction

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"[1]. Heads of organisations are obliged to take reasonable steps to ensure that they understand and operate within the Government's accountability framework, under directions issued by the Public Service Commissioner, pursuant to the *Public Service Act 1999*. The Public Service Commissioner suggests that organisations can "Demonstrate that due process has been followed in [their] actions and decisions through the existence and maintenance of good recordkeeping systems".

2. Definition of a Record

Records are evidence of business conducted by an organisation.

NDIA's records comprise both structured information, such as is captured in major business systems, and unstructured information, such as is created using office applications Microsoft *Word*, *Excel* and *Outlook* and is captured in the corporate recordkeeping system. Records can be in any form; however, NDIA primarily manages two types of records: physical and digital. Any reference within this policy to "a record" or "records" refers to both physical and digital records.

A physical record is any[2]
"…document (including any written or printed) or object (including a sound recording, coded storage device, magnetic tape or disc, microform, photograph, film, map, plan or model or a painting or other pictorial or graphic work) that is, or has been, kept by reason of any information or matter that it contains or can be obtained from it or by reason of its connection with any event, person, circumstance or thing."

digital records are[3]
"Records created, communicated and maintained by means of computer technology. They may be "born digital" (created using computer technology), or they may have been converted into digital form from their original format (e.g. a scanned rendition of a paper document)."

NDIA creates digital records in a variety of ways and may store them in many systems including databases and business information systems, shared folders, email applications and hard drives.

[1] APS Managing Official information, [Online],: http://www.apsc.gov.au/aps-employment-policy-and-advice/aps-values-and-code-of-conduct/aps-values-and-code-of-conduct-in-practice/managing-official-information accessed 3 September 2013

[2] Source: Archives Act 1983 Section 3 Interpretation http://www.austlii.edu.au/au/legis/cth/consol_act/aa198398/s3.html accessed 4 September 2013

[3] Source: Adapted from National Archives of Australia – Glossary [Online] Available: http://www.naa gov.au/records-management/publications/glossary.aspx#gloss-digitalrecord accessed 4 September 2013

The following list of digital records is not exhaustive, but highlights the range of digital records covered by this policy:

- electronic messages from communication systems such as email, windows messaging, SMS (Short Messaging Services), electronic document exchange (electronic fax), voice mail, and multimedia communications (e.g. Microsoft Office Communicator, video conferencing and teleconferencing);

- those created using office applications such as word-processed documents, spread sheets, presentations and desktop published documents;

- records generated by business information systems such as databases, human resources systems, financial systems, workflow systems, client management systems, systems developed in-house and content management systems; and

- records in online and web-based environments such as intranets, extranets, public websites and those created through online transactions.

3. Scope

This policy applies to all NDIA staff members and contract personnel; to all officers including those in National, State and Regional offices and remote locations; and those outsourced functions and statutory organisations falling under NDIA's responsibility.

It applies to all aspects of NDIA's business; all records created during business transactions; and all business applications and ICT systems used to create, store and manage records including email, database applications and websites.

This policy provides the overarching framework for any other corporate recordkeeping policies, instructions, practices or procedures which are provided on NDIA's intranet site.

Any external service provider, program office or client of NDIA that creates, holds, manages or maintains NDIA records on behalf of the department, when entering into a new agreement or contract with NDIA, must comply with this policy.

4. Legislation & Standards

NDIA is committed to complying with legislation and standards related to recordkeeping, access rights and the production of records including, but not limited to, the following:

- *National Disability Insurance Scheme Act 2013*
- *Public Governance, Performance and Accountability Act 2013*
- National Archives of Australia - Administrative Functions Disposal Authority (2010)
- *Archives Act 1983*
- *Archives Amendment Act 2008 disposal*
- *Audit Act 1901*

- *Audit Amendment Act 1979*
- *Audit (Transitional and Miscellaneous) Amendment Act 1997*
- *Auditor-General Act 1997*
- *Australian Standard AS ISO 15489*
- *Copyright Act 1968*
- *Crimes Act 1914*
- *Criminal Code Act 1995*
- *DIRKS [Designing and Implementing Record Keeping Systems] a Strategic Approach to Managing Business Information (2001)*
- *Evidence Act 1995*
- *Evidence Act (Transitional Provisions and Consequential Amendments) Act 1995*
- *Electronic Transaction Act 1999*
- *Freedom of Information Act 1982*
- *Work Health and Safety Act 2011*
- *Ombudsman Act 1976*
- *Privacy Act 1988*
- *Public Service Act 1999*
- Recordkeeping Metadata Standard for Commonwealth Public Authorities (Version 2.0 2008).

NDIA is also committed to ensuring that its recordkeeping systems comply with the *Australian Standard for Records Management AS ISO 15489 – 2002*, the National Archives of Australia's Digital Transition Policy, Digital Continuity Plan and Digital Continuity Principles suite of recordkeeping guidelines, standards and policies and the instructions set out in NDIA's *Protective Security Framework* and the *Information Security Manual*.

5. Recordkeeping Systems Policy Statement

All records of lasting value are to be captured and maintained through an appropriate recordkeeping system as soon as possible after creation. Records with particular context should be maintained by the most appropriate system for that type of record. For example, s47E(d) - certain operations of age [redacted]

Recordkeeping systems include not only the computer application but also the processes required to manage all records pertaining to them, regardless of their medium.

There is generally no reason to print and file in hard copy records that are created electronically, even if the document is likely to be required as evidence. Amendments to the *Evidence Act 1995* and the *Electronic Transactions Act 1999* mean electronic records are admissible as evidence.

Where possible, NDIA staff should capture electronic records in s47E(d) - certain [redacted] unless there is a business imperative to create a hard copy record.

Over time, NDIA's goal is to move to a fully compliant system that enables the formal creation, classification, and retention requirements of a record. s47E(d) - certain operations of agencies [redacted]

National disabilityinsurance Agency

compliant. Provision has been made for future NDIA's business systems to be hosted by DSS requiring that all managed records will comply with this policy and the following processes as a minimum:

- the **creation** and capture of records;
- the **storage** of records;
- the **protection** of record integrity and authenticity;
- the **security** of records;
- **access** to records; and
- the **disposal** of records in accordance with approved records authorities.

Each recordkeeping system is to have a business system owner.

s47E(d) - certain operations of agencies

The following systems are recognised as corporate recordkeeping systems for NDIA records:

s47E(d) - certain operations of agencies

National disabilityinsurance Agency

6. Disposal or Destruction of Records

NDIA's records are regarded as Commonwealth records and can only be disposed of in accordance with the various provisions of the *Archives Act 1983*, including normal administrative practice (NAP). Staff members should take care not to unintentionally dispose of a Commonwealth record outside of these provisions. Inappropriate and unlawful disposal is an offence under the *Archives Act 1983*, and a breach of the APS Code of Conduct[4].

7. Responsibilities

The Chief Executive Officer has nominated the Branch Manager, Business Services Innovation Branch, as the senior officer responsible for recordkeeping policy and standards in NDIA.

The Chief Executive Officer is authorised to grant special access to Commonwealth records in accordance with s56(2) of the *Archives Act 1983* for NDIA.

NDIA as an organisation is responsible for:

- setting up sound recordkeeping systems, based on identified recordkeeping requirements and including such elements as written policy and guidelines and training of users;
- making sure proper and accurate records are created, maintained, kept and documented within these systems;
- ensuring that the records remain useable and are not prematurely destroyed; and
- ensuring that public access to records is given when legitimately required and, conversely, that records are not inappropriately accessed.

NDIA staff members, including contractors and consultants, are to ensure that appropriate records are created and captured for all the business functions, activities and transactions they are involved with. Staff members are required to appropriately classify and store information as set out in the Recordkeeping Procedures[5]. Emails received in the course of business are records and should be managed appropriately[6].

---

[4] Source: http://www.apsc.gov.au/aps-employment-policy-and-advice/aps-values-and-code-of-conduct/aps-values-and-code-of-conduct-in-practice/managing-official-information Accessed 3 September 2013

[5] Source: FaHCSIA's Recordkeeping Procedures

[6] Source: FaHCSIA's Internet Governance Framework.p.8 http://staffnet/waf/it/websites/Documents/Internet-Governance-Framework.docx and, ICT Security Policy 2012 accessed 4 September 2013 http://staffnet/waf/it/corpsystems/Documents/ICT_security_policy.pdf accessed 4 September 2013

Staff members should not store official records and emails in personal locations and in systems that do not have recordkeeping functionality. Where an appropriate record does not exist (such as following a phone conversation or meeting) a record shall be created and lodged in a recordkeeping system. Staff members are required to comply with disposal procedures, follow work area procedures and use records to meet the organisation's recordkeeping obligations.

The Cross Portfolio & Information Branch has responsibility for managing the NDIA's records and provides recordkeeping services to NDIA. NDIA's Records Manager has the delegation to approve the appropriate disposal of NDIA records.

Responsibilities are shown in the NDIA's Recordkeeping Responsibilities Matrix at the end of this document.

Ethical Behaviour in Practice

As NDIA employees we are bound by NDIA Values and the APS Values and Code of Conduct to act ethically in relation to all things that we do in connection with our employment.

Ethical behaviour encompasses the concepts of honesty, integrity, transparency, probity, diligence, fairness, trust, respect and consistency. Ethical behaviour identifies and avoids conflicts of interest and improper use of our position or role as APS and NDIA employees.

Ethical behaviour ensures that NDIA business is conducted fairly, reasonably and with integrity. In all aspects of NDIA business, we need to ensure that we:

- recognise and avoid perceived or actual conflicts of interests;
- seek appropriate advice when dealing with probity issues;
- are accountable for, and can demonstrate accountability in our use of NDIA assets and property;
- comply with privacy laws and principles in the handling and release of personal information;
- do not accept inappropriate gifts or hospitality;
- comply with legislative requirements and NDIA policy, procedures and instructions;
- treat everyone with respect and courtesy;
- do not release official information without approval;
- take action immediately when we observe unethical behaviour;

- all of our dealings with our fellow employees, members of the public, private companies or organisations and other APS agencies are fair, transparent and even-handed; and

- decisions we make are evidence based and can withstand external scrutiny.

Actions which do not meet the ethical standards outlined above reflect poorly on NDIA and may constitute a breach of the APS Code of Conduct. In some cases unethical behaviour may also contravene Commonwealth legislation and lead to criminal prosecution.

For more information contact or refer to the:
NDIA's Workplace Relations Team in People Branch in relation to the APS Values and Code of Conduct;
Australian Public Service Commission's (APSC) Ethics Advisory Service – refer http://www.apsc.gov.au/ethics ;
APSC's "Reflect" decision making model – refer http://www.apsc.gov.au/publications-and-media/current-publications/reflect ; and
NDIA's Compliance Branch Fraud Prevention and Detection in relation to suspected Fraud.

NDIA related documents FIRSt ref: 26536915v1

Linked to documents:

s47E(d) - certain operations of agencies

Records Management - Legislation and Standards
NDIS Data Management Strategy 2012 – 2015
NDIS Data Migration Strategy 2013

Relevant Standards related to Records Management

- Protective Security Policy Framework (PSPF)
- AS/ISO 15489 Records Management Standard
- ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments
- ISO 31000:2009 Risk Management Standard
- AS 5044:2010 Australian Government Recordkeeping Metadata Standard (AGRkMS) Version 2.0
- Data Management Body of Knowledge - Data Management International Standards (DAMA)
- AS/NZS ISO/IEC 27001:2006 Australian Government Information Security Manual (ISM)
- HB 167:2006 Handbook on Risk Management[7]
- ISO 16175-2:2011 – Information and documentation
- AS 5090: Work process analysis for recordkeeping[8]

[7] Attorney Generals Department http://www ag gov.au/NationalSecurity/ProtectiveSecurityTraining/Pages/default.aspx 4 September 2013

[8] NAA Standards http://www.naa.gov.au/records-management/strategic-information/standards/ASISOstandards.aspx Accessed 4 September 2013

National disabilityinsurance Agency

Roles and Responsibilities Matrix

Responsibility	Roles									
	CEO	COO	Chief Information Officer	Business Systems Owners	General Managers	Branch Managers	Section Managers	Branch Manager Audit and Fraud	Staff Members	Records Manager
Risk Management										
Undertake appropriate risk analysis considering such areas as security, integrity, privacy and business continuity, and ensure that the outcomes are effectively implemented			✓	✓						✓
Governance										
Establish a governance structure to ensure that the requirements of this Policy are fulfilled	✓		✓							✓
Establish a governance structure to ensure that the operational requirements of recordkeeping are adequately addressed		✓								
Quality Assurance/Audit										
Establish appropriate quality assurance processes to ensure compliance with this Policy			✓					✓		✓
Establish appropriate quality assurance processes to ensure that recordkeeping is adequate				✓						✓
Delegations										
Designate a business system owner for each approved recordkeeping system			✓							
Authorise each approved recordkeeping system			✓							
Promulgate the approved recordkeeping systems			✓							
Authorise the disposal/destruction of records										✓

Responsibility	Roles

National disabilityinsurance Agency

	Chief Information Officer	Business Systems Owners	General Managers	Branch Managers	Section Managers	Branch Manager Audit and Fraud	Staff Members	Records Manager
Recordkeeping								
Develop and maintain Recordkeeping policy and procedures								✓
Accountable for Group's compliance with this Policy			✓					
Establish a framework for the capture and management of records for each recordkeeping system		✓	✓	✓	✓			
Ensure that staff members are creating records in accordance with the established frameworks			✓	✓	✓			
Ensure staff members are aware of the recordkeeping responsibilities that relate to their position			✓	✓	✓			
Responsible for records controlled by staff members under their supervision			✓	✓	✓			
Create full and accurate records of their activities in accordance with the established frameworks							✓	

National disabilityinsurance Agency

Bibliography

The following references were used in the preparation of this document:

- National Archives of Australia, Developing a Recordkeeping Policy (http://www.naa.gov.au/records-management/strategic-information/information-governance/key-documents/policy.aspx)
- National Archives of Australia, Digital Records (http://www.naa.gov.au/records-management/agency/digital/index.aspx)
- DSS ICT Security Policy
- Commonwealth Information Security Manual - 2009 accessed 3 September 2013
- Commonwealth Protective Security Manual - 2000
- Australian Standard for Records Management AS ISO 15489 - 2002
- Public Service and Merit Protection Commission, Values in the APS (http://www.apsc.gov.au/merit/the-merit-protection-commissioner-role) accessed 3 September 2013
- Council of Australasian Archives and Records Authorities, Policy Statement 7, Principles on Full and Accurate Records (http://www.caara.org.au/index.php/policy-statements/principles-on-full-and-accurate-records/) accessed 3 September 2013

NDIA

Policy – Information and Records Management Normal Administrative Practice (NAP)

Draft October 2018

ndis.gov.au

Overview:

Release	2
Effective Date	01/11/2018
Author	s22(1)(a)(ii) - Information and Records Manager, Information and Records Team.
Owner	Chief Financial Officer (CFO).
Client	National Disability Insurance Agency (NDIA). This includes Partners, employees, contractors and consultants.
Document Number	NED18/201384 Draft 2.01 (previously Doc. No. 32078239v3)

Version Control:

Version	Date	Author	Description of Changes
0.1	12/10/2018	s22(1)(a)(ii) -	First draft
1.02	26/11/2018	s22(1)(a)(ii)	NDIA - Senior Lawyer, Legal Branch, Governance Division

Endorsements

Version	Date	Name	Position
Doc. No. 32078239v3	27 August 2014	s22(1)(a)(ii) -	Special Counsel - Public Law
Doc. No. 32078239v3	22 September 2014	s22(1)(a)(ii) -	NAA – Assistant Director, Agency Accountability

Approvals

Version	Date	Name	Position
2.00		Victor Walter	Deputy CEO, Corporate Services and CFO
2.00		Melissa Woodburn	General Manager, Finance and Corporate Services

Table of Contents

1. Definitions

The following definitions from the AS ISO 15489:2017 Records Management Standard to provide context:

Definition	Definition Description
Activity	Major task performed by a business entity as part of a *function* (see function).
Conversion	Process of changing records from one format to another.
Destruction	Process of eliminating or deleting a record, beyond any possible reconstruction.
Disposition	Range of processes associated with implementing records retention, *destruction* or transfer decisions which are documented in *disposition authorities (records authorities)* or other instruments.
Evidence	documentation of a *transaction* [SOURCE: ISO 30300:2011, 3.1.5] Note 1 to entry: This is proof of a business transaction which can be shown to have been created in the normal course of business activity and which is inviolate and complete. It is not limited to the legal sense of the term.
Function	Group of activities that fulfils the major responsibilities for achieving the strategic goals of a business entity.
Metadata for records	Structured or semi-structured information, which enables the creation, management, and use of records through time and within and across domains Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time.
Migration	The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and useability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another. Process of moving records from one hardware or software configuration to another without changing the format [SOURCE: ISO 30300:2011, 3.3.8].
Record(s)	Information created, received and maintained as *evidence* and as an asset by an organization or person, in pursuit of legal obligations or in the *transaction*) of business.
Records authority (Disposition Authority)	Instrument that defines the *disposition* actions that are authorised for specified records.
Records management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and *disposition* of records, including processes for capturing and maintaining *evidence* of and information about business activities and *transactions* in the form of records.
Records (Information) system	Information system which captures, manages and provides *access* to records over time Note 1 to entry: A records system can consist of technical elements such as software, which may be designed specifically for managing records or for some other business purpose, and non-technical elements including policy, procedures, people and other agents, and assigned responsibilities.
Schema	Logical plan showing the relationships between metadata elements, normally through establishing rules for the use and management of metadata specifically as regards the semantics, the syntax and the optionality (obligation level) of values [SOURCE: ISO 23081-1:2006, 3.3].
Transaction	Smallest unit of a *work process* consisting of an exchange between two or more participants or systems [SOURCE: ISO/TR 26122:2012, 3.5]
Work process	One or more sequences of actions required to produce an outcome that complies with governing rules [SOURCE: ISO/TR 26122:2012, 3.6].

2. Introduction

The National Disability Insurance Scheme (NDIS) is the Australian Government's policy to address the rights and entitlements of eligible vulnerable Australian citizens with disability in accordance with Australia's obligations under the United Nations (UN) Convention on the Rights of Persons with Disabilities.

The National Disability Insurance Agency (NDIA) is the independent Commonwealth entity responsible for implementing the NDIS to improve life for Australians with disability, their families and carers. The NDIA is accountable to the Australian Government through the Minister for Social Services and the Council of Australian Governments (COAG) Standing Council on Disability Reform. The NDIA operates under the National Disability Insurance Scheme Act 2013 (NDIS Act) and receives funds contributed by the Australian Government, states and territories. The NDIA is committed to establishing and maintaining information management practices that meet its business needs, accountability requirements and stakeholder expectations..

Normal administrative practice (NAP) relates to low level information without ongoing business value that can be routinely destroy information that is **not needed as documented evidence** of the NDIA's business decision making processes, that are not assets and are therefore not needed to form part of its corporate or operations business recordkeeping systems.

Records[1] are evidence of business activity and information assets and are enablers of business providing a factual knowledge base both current and strategic.[2]

2.1 Purpose

The purpose of this policy is to clarify responsibilities and to advise NDIA staff, contractors and consultants, Partners and contractors what information can be routinely destroyed in the normal course of business. It is to provide guidelines to assist the NDIA with an appropriate tool to remove or destroy transitory or ephemeral information considered to have no ongoing business or government value, or reduplicated information such as 'copies of copies' and unsolicited advertising material. This policy NAP is a *process* by which certain documents and information (electronic, paper and other formats) can be removed or destroyed without reference to authorised National Archives of Australia's (NAA) Records Authorities.

Section 24 of the *Archives Act 1983*, provides that Commonwealth agency records can be destroyed:

- As required by a specific law;
- With the permission of the National Archives of Australia using a Records Authority; or
- In accordance with a normal administrative practice (NAP).

The benefits of complaince with this policy include more efficient work practices and the management of retained information as a business asset.

2.2 Policy Statement

NAP relates to the National Disability Insurance Agency's (NDIA's) certain low value and short-term information where there is a low level of risk.

The NDIA recognises its regulatory requirements as a Commonwealth agency, inclusive of Partner obligations under the Archives Act 1983 related to legal destruction and retention of government information and records. Use of a normal administrative practice for destroying information is permitted under the ***Archives Act 1983*** section 24(2)(c)[3].

[1] Archives Act : Record means a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of: (a) any information or matter that it contains or that can be obtained from it; or (b) its connection with any event, person, circumstance or thing.

[3] Archives Act 1983 S.24 Disposal, destruction etc. of Commonweatlh records

NAP covers records[4] that do not document business decisions and where the risk to the agency associated with their destruction is low.

This policy applies to NDIA employees, contractors, consultants, Partners and staff related to information that can be routinely destroyed when not needed to provide evidence of business decisions. It is important to follow the process set out in this statement as original documents may need to be provided as evidence in court or tribunal proceedings and are therefore their absence is high risk.

This Policy is to be read in conjunction with NDIA's strategic framework including the NDIA Information and Records Management Policy, the National Disability Insurance Scheme (NDIS) Records Authority and the Commonwealth General and Administrative Records Authorities[5].

2.3 Risk considerations

Deciding if a record can be destroyed using NAP can only be done with a cultural understanding of the NDIA business the NDIS. If you do not have an understanding of the business context in which the documents and records were created, you are not in a position to decide if the documents have (or do not have) ongoing value and whether NAP can be applied.

Business areas should identify and advise staff of the kinds of records associated with their business activities to which NAP for destruction can apply.

The responsibility of using NAP to delete documentation (information contained in software and systems, or on paper) lies with each staff member, Partner or contractor using this policy as an avenue for destruction. It is the responsibility of each staff member, Partner or contractor to utilise NAP within its intended boundaries.

Destruction beyond the limitations of NAP constitutes unlawful destruction of records.

2.3.1 Delete with confidence

- Non-business information such as personal unofficial emails, spam, unsolicited junk mail like 'hot offers', non-business related material.
- Duplicates of information that has already been saved into authorised recordkeeping systems or another business information system.
- External publications, catalogues and offers.
- Reference copies (not master copies) of newsletters, procedures, guidelines, manuals, policies.

2.3.2 Needs consideration

- Low-risk emails such as system reminders and alerts, discussion lists and RSS feeds, duplicate emails kept for reference purposes, parts of an email thread where the full thread is saved into the HPRM or authorised business information systems, 'for your information' communications, email bounce backs.
- Invitations, diaries and calendars (with the exception of SES)
- Duplicate copies of NDIA's publications and promotional material.
    - Note: the business area responsible for the publication has responsibilities to keep master copies.
- Drafts, rough or routine calculations and working papers.
- Business information held in shared work spaces such as shared drives and business systems.

---

[4] NAA Glossary: A record is all information created, sent and received in the course of carrying out the business of your agency. Records have many formats, including paper and electronic. Records provide proof of what happened, when it happened and who made decisions. Not all records are of equal importance or need to be kept. *Adapted from: Archives Act 1983, Part I, Section 3; Standards Australia, AS-ISO 15489, Part 1, Clause 3.15.*Accesssed 23 September 2014

[5] NAA: Authorities covering common business activities accessed 9 February 2017

- Documents prepared with the involvement of senior staff; these are often important and may not be appropriate for destruction using NAP.

2.3.3 Do not delete

Valuable business information that is required:

- for accountability purposes
- for the ongoing efficient administration of agency business
- to protect rights and entitlements of individuals, groups, or the Government, or
- because of its cultural or historical value, or to meet community expectations.

2.4 Scope

This policy applies to all NDIA staff, Partners, and contractors who are working with NDIS Commonwealth Government information, all aspects of NDIA's business and all information, records and data regardless of format, created during business transactions.

This policy applies to information in all formats including documents, email, voice messages, audio-visual materials and data in business systems (e.g. websites, Outlook, social media applications, databases) that will not be required as evidence of business activity.

Any information in hard copy or digital format, such as printed out or reduplicated material 'copies of copies', or low value drafts, must be destroyed in a protected method in line with the NDIA's ICT Information Security Policy. For example, drafts and printed copies of NDIA/NDIS information must only be disposed of by shredding and/or placing in security bins. The ICT Security Advisor (ITSA) can provide specific advice regarding the sanitisation and/or disposal of IT equipment used for NDIS information such as scanning equipment, portable storage devices.

3. NAP Exceptions – do not delete

The following information **cannot** be destroyed under NAP:

- Policy drafts and working papers
- Report drafts and working papers
- Review drafts and working papers
- Research working papers
- Standards and guidelines working papers
- Working papers for the development of whole-of-government procedures
- Working papers for records transfers and sentencing
- System logs which are used to show a history of access or change to data (e.g. system access logs, internet access logs, system change logs and audit trails etc.)
- Records documenting the migration of records between electronic systems and from one electronic medium to another. Includes strategies for the migration and quality assurance checks to confirm accuracy of the migration process
- Information that is likely to be required as evidence in current or future legal proceedings
- Information that is required to be kept by law (including by a records authority or disposal freeze)
- Information that is required to be kept under an agency policy, procedure or guideline
- Information that is a draft of a Cabinet or ministerial submission
- Information that is a draft of an agreement or other legal document
- Information that is needed to document a significant issue
- Information that is needed to clarify, support or give context to an existing record
- Information that is needed to show how a decision was made
- Information that is needed to show when or where an event happened
- Information that is needed because it indicates who made the decision or gave the advice
- Information that is needed because it contains information on the rights, privileges or obligations of government, organisations or private individuals

- Information that is a draft or working paper that contains decisions, reasons, actions and/or significant or substantial information where this information is not contained in later documents or the document remains not finished.
- Records that are linked to community expectations providing rights and entitlements for participants.
- Records that are needed because they contain information on the obligations of government, organisations such as partners, service providers.
- Information related to the rights and entitlements of people with disabilities, their carers and family members and other private individuals.
- Information that is a draft or working paper that contains decisions, reasons, actions and/or significant or substantial information where this information is not contained in later documents, or entered in the NDIA's business and records management systems, or the document remains unfinalised.
- Information that provides support to the ongoing efficient administration of NDIA's business.
- Records considered as having cultural, social or known historical value.
- Physical paperwork that is scanned or reimaged. See the NAA's General Records Authority 31 (GRA31)[6] .
- Diaries and meeting attendance used to record important matters that may be required as evidence belonging to staff holding high or high profile positions, for example the
    - Board
    - Chief Executive Officer
    - SES Band
    - State/Regional Manager
    - Contractor / Consultant meetings and presentations
    - Meetings and appointments between Planners, Partners, Local Area Coordinators related to appointments with potential participants.

- Drafts, calculations and working papers, e.g. drafts that contain significant or substantial changes or annotations, and document business activities.
- Information and records held in shared work spaces such as shared drives and business systems (that should be transferred to a business system, after evaluation against applicable Records Authorities.
- Items registered in the NDIA's business and records management systems which can only be removed by the System Administrator with approval from the Information and Records Advisory Unit.
- Documents prepared with the involvement of senior staff and associated versions showing the decision making processes; these are often important it may not be appropriate for destruction using NAP.

Where a NAP exception applies, or if there is any uncertainty concerning whether the record should be kept keep the record and place it in the NDIA's business and records management systems. If you are unsure about any of these contact the Information and Records Advisory Team before destroying the information.

4. Agency Publications and Promotional Material

Place one copy in the appropriate and approved NDIA records management system and lodge one copy with the National Library of Australia in accordance with the legal deposit requirements in National Archives of Australia AFDA Express – Publication.

5. Metadata about records

Metadata associated with deleted records will be retained in the NDIA records management systems and retained as a National Archive Information Management (under class 1490 of the AFDA).

[6] General Records Authority (GRA31)

6. Roles and Responsibilities

All NDIA staff, consultants and contractors, Partners and contractors that manage NDIA Commonwealth Government records must:

- Be familiar with the NDIA NAP guidance and understand their personal obligations and responsibilities when using NAP;
- Understand their personal obligations and responsibilities when using NAP ;
- Destroy information and records that clearly meet the NAP policy criteria when they are no longer required for business purposes;
- Ensure that where information and records are identified for destruction under NAP, the method of destruction employed is appropriate to the security classification of the record content; and
- Seek guidance from NDIA Information Manager if there is any uncertainty over the applicability of the NAP to their information or records:

Role	Responsibility
Deputy Chief Executive Officer (DCEO) – Corporate Services and Chief Financial Officer	Ensures that the NAP policy is adequate to meet the needs and risks of the NDIS and is consistent with the Information and Record Management Policy and the NDIA Information and Records Management Strategy and Implementation Plan (currently in draft); Ensures that adequate guidance is produced to support NDIA staff, LAC Partners, Contractors and outsourced providers in understanding and implementing the NAP policy to Commonwealth information; and Reviews and revises the NAP policy and guidance as required to ensure they remain appropriate.
All Managers and supervisors of NDIA staff, Partners and contractors	Promote understanding and use of the NDIA NAP Policy to staff, Partners and contractors under their supervision through the use of NAP guidance; Incorporate NAP policy directives into their business unit work procedures, where appropriate; Liaise with the NDIA Information Manager in relation to using the NAP Policy, any barriers to its use and advise the NDIA Information Manager of any changes in the business environment which would impact on information and records management requirements, such as new areas of business that need to be covered by a records authority; Encourage and support staff and contractors in the compliant destruction of records that are eligible for destruction under the NAP policy once they are no longer required for business purposes; and Monitor staff and contractors under their supervision to ensure that they understand and comply with the NAP policy and guidance.
All Contractor Managers	Are responsible for the insertion of recordkeeping provisions (including NAP) into agency contracts with outsourced providers and contractors; and Regularly monitor outsourced service providers and contractors with whom they have a contract to ensure that they understand and comply with the NAP policy and guidance.
All ICT Staff and NDIA business system owners	Assist in incorporating NAP policy into the design and development of the NDIA's business information systems, including records management and IT systems; and Ensure that any actions, such as data migration strategies, removing data from systems, email, storage or folders, are undertaken in accordance with this and other relevant policies
NDIA Information Manager	Disseminate the NDIA NAP policy and guidance to all NDIA staff, LAC Partners, Contractors and outsourced providers; Delivers training and advice to all staff on the appropriate implementation of the NDIA NAP policy, including induction sessions for new staff;

	Encourages the incorporation of NAP policy directives into business unit work procedures; and Ensures that the NDIA NAP policy is incorporated into the development of the NDIA's recordkeeping systems, including business and IT systems; Monitors compliance with the NAP policy.

7. Communication and Training

All staff will be provided with training on aspects of the NAP policy. Training will be relevant to roles and positions, current, and provided on annual basis. Training will be tailored so that it is meaningful to different workgroups managing Commonwealth and NDIS information and in the NDIA.

8. Monitoring and Review

The DCEO, will review this policy every three (3) years, or earlier if required.

- Staff with responsibilities for NDIA information and records management will monitor the compliance with the NAP policy.
- Supervisors and managers will monitor their respective staff and contractors to ensure the NAP policy is implemented correctly.
- Contract managers will monitor compliance of contractors and outsourced service providers with the NAP Policy.
- Compliance with this policy will be monitored by the information and records management unit with the support of workplace supervisors. Levels of compliance will be reported at least annually to senior management.

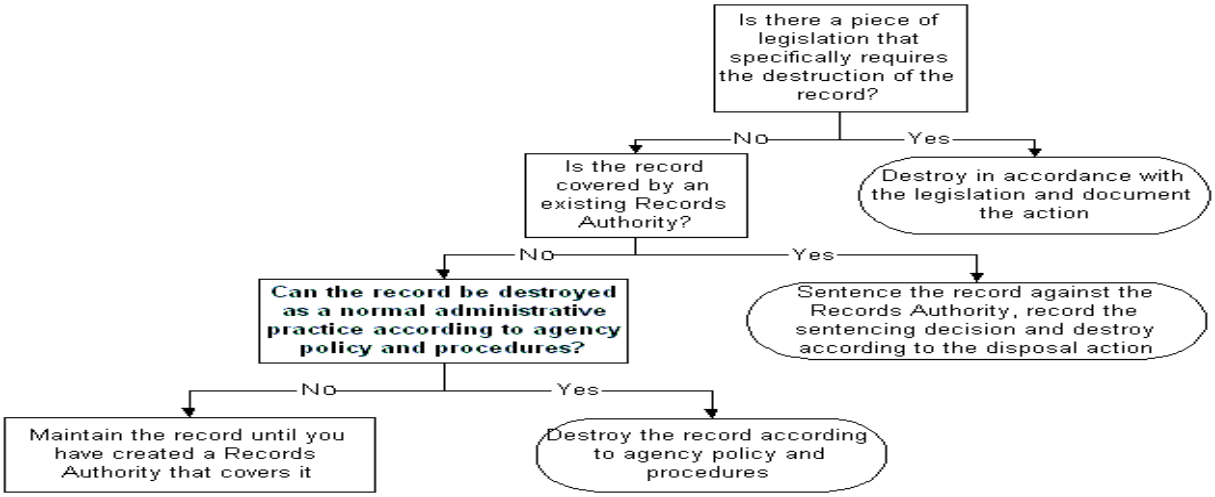
9. Resources

NAA: Destroying records as a normal administrative practice.

The following flowchart illustrates the analysis required when deciding if you can destroy information using a NAP.[7] Please refer to an appropriate Records Authority or request assistance from the Information and Records Management team.

Authorised Records Authorities are instruments that have been previously well-defined in accordance with appropriate legislation with adequate requirements for retention of information. Alternatively contact the NDIA Information Manager for assistance.

[7] NAA: flowchart accessed on line 24 May 2017


Is there a piece of legislation that specifically requires the destruction of the record?
No
Yes
Destroy in accordance with the legislation and document the action
Is the record covered by an existing Records Authority?
No
Yes
Sentence the record against the Records Authority, record the sentencing decision and destroy according to the disposal action
Can the record be destroyed as a normal administrative practice according to agency policy and procedures?
No
Yes
Maintain the record until you have created a Records Authority that covers it
Destroy the record according to agency policy and procedures