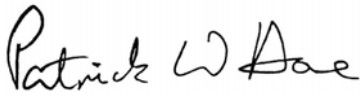
Records Management Policy

Managing Director's authorisation:



Effective date: 30 April 2018

TABLE OF CONTENTS

1. PURPOSE

The purpose of this policy is to provide direction to employees on the creation, maintenance, storage and disposal of FRDC records and associated metadata.

2. RESPONSIBILITY

Responsibility for this policy resides with the General Manager Business.

3. DEFINITIONS AND ACRONYMS

Definitions - follow link to Definitions
Acronyms – follow link to Acronyms and Abbreviations

4. RISK CATEGORY

Compliance	Financial	Governance	ICT	People	Research
☐	☐	☒	☐	☐	☐

5. RELEVANT DOCUMENTATION

This section contains links to internally and externally facing documents – access to internally facing documents is restricted to FRDC employees.

Relevant documentation	Document location or web address
Internal	
Information Management Policy	NEMO-17805-61
Records management procedure	NEMO-29-1565
External	
Archives Act 1983	Archives Act
Australian Government Recordkeeping Metadata Standard	NAA
Crimes Act 1914	Crimes Act
Digital Continuity Policy (NAA) 2020	Digital continuity policy
Freedom of Information Act 1982	FOI Act
NAA's Normal Administrative Practice (NAP)	NAP
Privacy Act 1988	Privacy Act
Protective Security Policy	Protective security policy
Information Governance Framework	Information Governance Framework

6. PUBLICATION

This policy is to be made available on the FRDC website.
This policy is not to be made available on the directors' site.

7. BACKGROUND

FRDC's records are its corporate memory and a vital asset for ongoing accountability. Good recordkeeping is critical to corporate governance and operational efficiency, provides essential evidence of business activities and transactions, and demonstrates accountability and transparency in FRDC's decision-making processes

This policy applies to all records and associated metadata from the time of creation or capture and covers:

- all FRDC employees, regardless of employment type
- all aspects of FRDC's business operations
- all types and formats of records created to support business activities
- all business applications used to create records
- organisations and businesses, including their employees, to which FRDC has outsourced its functions or activities, and therefore associated recordkeeping responsibilities

This policy does not relate to records created by any other agencies, except where they form part of a FRDC business transaction.

This policy, together with the Information Management Policy (see relevant documentation), ensures that complete and accurate records of FRDC's business activities are available and accessible for as long as required for operational, accountability and compliance purposes.

The Retention and disposal schedule (see Records management procedure) supporting this policy is intended to ensure that FRDC undertakes best practice records management.

8. POLICY

FRDC will comply with its legislative and regulatory requirements under the Archives Act 1983. FRDC is committed to meeting the principles and practices set out in the following whole-of-Government policies and standards endorsed by the National Archives of Australia (NAA):

- the whole-of-Government Digital Transition Policy
- the whole-of-Government Digital Continuity Policy
- the International and Australian Standard for Records Management (ISO 15489) – as supporting and guiding principles
- the AGLS Metadata Standard – where applicable

All employees and contractors, will be responsible for recordkeeping.
All employees and contractors will be aware of their obligations under this policy and take reasonable action to ensure ongoing compliance.

8.1 Definition of a Record

Records are evidence of business conducted by an organisation. Any reference to a record in this policy refers to records in any format as defined in the Archives Act 1983. The approved Retention and Disposal Schedule (see Records management procedure) highlights characteristics that differentiate a record from other types of information and provide for a record to be admissible as evidence.

FRDC employees are responsible for keeping a record of business transactions conducted as part of their duties. Examples of business transactions include documenting actions, events, conversations or other transactions where they provide

evidence of formal advice or directions, or significant decisions. Records can be in any format. This includes but is not limited to:

- hard copy or electronic documents
- paper or electronic files
- electronic messaging
- social media
- web content
- photographs
- videos
- data in business systems
- models, plans and architectural drawings

For a record in digital format to be meaningful and to serve as admissible evidence of a business transaction, associated metadata needs to be captured or created with the record to provide adequate context and to support its authenticity and management over time. Along with other provisions, as set out in the relevant areas of this policy, minimum metadata standards set by the NAA in the Australian Government Recordkeeping Metadata Standard are to be met. This will help to ensure that FRDC's business, accountability and archival requirements are met in a systematic and consistent way, and that digital records are described, reliable, meaningful, admissible as evidence, accessible, sharable and re-usable for as long as they need to be retained.

8.2 Authorised Recordkeeping Systems

FRDC ensures its systems and applications are compliant for records keeping purposes. To this end, each application/platform is audited to reinforce the management of both physical and electronic records (documents and files/containers) along with the required associated metadata.

Exclusions: FRDC information (irrespective of format) stored in shared drives, personal drives, email and on backup disks or drives are not 100% compliant with FRDC's recordkeeping obligations. These mediums and locations do not capture sufficient metadata to meet the legal recordkeeping retention and disposal requirements, and/or do not allow records to be widely searchable or accessible to all who need them, are not authenticated and are not secure from alteration or deletion.

This business information remains non-compliant until it is registered/captured as a record in an authorised business system as outlined by FRDC. Shared network drives are not authorised for the storage and management of records.

A Business Information System (BIS) is an information reporting and/or transaction system used within FRDC. Business information systems are not automatically records management compliant – they contain structured data that potentially constitutes part of a record but this does not by default contain the contextual information to ensure reliability, authenticity and usability. Further, legal recordkeeping retention and disposal requirements (beyond keeping backups of data) are usually not adequately catered for.

Authorised business information systems, which comply to records management requirements for FRDC need to:

- be capable of collecting all information required for the activity – it should be fit for purpose
- be capable of capturing content, structure and context of the record
- provide adequate and compliant storage of records
- provide protection of record integrity and authenticity
- ensure the security of records
- be readily accessible to all employees who need to use the records contained within the system, for as long as the record is needed
- undertake the disposal of records in accordance with approved disposal schedules
- ensure the recoverability of records in the event of a disaster
- ensure the availability of records in a useable format through technology changes and migration

8.3 Access to Records

Under provisions of the Archives Act 1983, Freedom of Information 1982 and Privacy Act 1988, records created in FRDC can be released to the public on request, if they meet certain criteria. Failure to maintain or locate reliable records when requested, may lead to lost revenue or excessive retrieval costs, legal action or reputational damage for FRDC.

The Privacy Act 1988 governs the collection, use and disclosure of information about individuals to ensure that the information collected directly relates to an agency's functions. Under the Privacy Act, members of the public have the right to access records about themselves that are less than 30 years old.

8.4 Security of Records

Information security includes measures such as procedures for the handling, storage and disposal of official information, and information communications and technology controls. This policy should be read in conjunction with the Australian Government Protective Security Manual and the FRDC Information Management policy (see relevant documentation).

FRDC employees should note the following when creating, storing, retrieving, editing and circulating information:

- employees must ensure that they apply the correct security classification to each document at the time of creation, and save this document in an appropriate location.
- employees should avoid restricting access to named users, and instead use positions, roles or groups wherever practical.
- it is the responsibility of individual users to ensure that security and access controls on documents remain appropriate and in line with the need-to-know

principle, as documents are edited, emailed, shared, and to cater for potential changes over time.

- documents should be sent within FRDC as a link from the source system rather than as an attached document wherever possible, allowing the inherent security and access controls to manage whether the recipient has access.
- particular care should be given to the access controls applied to documents where privacy issues are involved.

8.5 Disposal, Deletion or Destruction of Records

It is an offence to dispose of, delete or destroy any FRDC record without authorisation from the NAA. Under the Archives Act 1983 and the Crimes Act 1914, FRDC records cannot be disposed of other than in accordance with the approved NAA disposal authorities.

Records created and received as part of FRDC'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 owner, using the appropriate method, without seeking formal authorisation.

9. ATTACHMENTS

#	Description
1	Not applicable