

## Data Management Procedure

**General Manager's Authorisation**

**Effective Date**

Kyaw Kyaw Soe Hlaing



2 April 2025

### Contents

1. PURPOSE.....	3
2. RESPONSIBILITY .....	3
3. DEFINITIONS, ACRONYMS AND ABBREVIATIONS.....	3
4. RISK CATEGORY .....	4
5. RELEVANT DOCUMENTATION.....	4
6. TRAINING .....	5
7. PUBLICATION .....	5
8. ACTIONS.....	5
9. ATTACHMENTS.....	5
Attachment 1 FRDC Data Governance Framework .....	6
PURPOSE.....	6
DOCUMENT MANAGEMENT.....	7
GENERAL .....	7
Overview .....	7
Principles .....	8
PRINCIPLE 1. Transparent, clear and honest collection, use and sharing of data .....	8
PRINCIPLE 2. Fair and equitable use of data.....	9
PRINCIPLE 3. Ability to control and access data .....	9
PRINCIPLE 4. Documentation and Record Keeping .....	10
PRINCIPLE 5. Portability of Data .....	10
PRINCIPLE 6. Keeping Data Secure .....	10
PRINCIPLE 7. Compliance with National and International Laws.....	10
Roles & Responsibilities.....	11
DATA GOVERNANCE ROLE 1. Chief Data Officer .....	11
DATA GOVERNANCE ROLE 2 Data Steward.....	11
DATA GOVERNANCE ROLE 3 Data Provider .....	12
DATA GOVERNANCE ROLE 4 Data Users.....	12

**Version: 2**

**Review date: 1/10/2027**

**Document ID: NEMO-759100797-84**

Managing Data.....	14
DATA MANAGEMENT ASPECT 1 Data Collection .....	14
DATA MANAGEMENT ASPECT 2 Data Quality .....	14
DATA MANAGEMENT ASPECT 3 Data Classification.....	15
DATA MANAGEMENT ASPECT 4 Data Access .....	17
DATA MANAGEMENT ASPECT 5 Data Sharing .....	18
DATA MANAGEMENT ASPECT 6 Data Storage .....	19
DATA MANAGEMENT ASPECT 7 Data Security.....	19
DATA MANAGEMENT ASPECT 8 Data Use .....	19
DATA MANAGEMENT ASPECT 9 Data Disposal.....	20
What does successful Data Governance look like? .....	21
Attachment 2 Data Governance on a Page.....	22

## 1. PURPOSE

This procedure describes the method for managing data that arises from FRDC's core business. This procedure does not address matters related to corporate information, such as: management of personnel and financial records; meeting papers and minutes; correspondence and emails; or intranet content.

## 2. RESPONSIBILITY

Responsibility for this procedure resides with General Manager ICT & Digitalisation

Data informs decisions throughout all business units within the FRDC and as such, this framework applies to the entire organisation. Specific Data Governance Roles & Responsibilities are described under the Data Governance Framework below

The scope of this policy is activities conducted by FRDC and does not extend to our research partners. Technology and research partners contracted by FRDC should have or as part of the terms of their contract be encouraged to implement adequate policies and obtain the relevant certifications in the provision of their services to FRDC.

## 3. DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Definitions link [Definitions](#)

Acronyms Link [Acronyms and Abbreviations](#)

Term	Definition
Data	Data are measurements and observations, including facts, figures, records, statistics or opinions, whether true or not, that have been collected directly or obtained as a by-product of a compliance, regulatory or service-delivery process
Data management	Covers a broad range of activities and concepts including data ownership/ data documentation (metadata)/ data quality, data custodianship/ data access and dissemination/ and data security
FRDC Data	FRDC Data is defined as all data originated by FRDC. This includes <ul style="list-style-type: none"> <li>• Financial datasets (including MYOB, excel etc).</li> <li>• Human Resources and Payroll datasets.</li> <li>• Documents and Spreadsheets (MS Word, PDF, text).</li> <li>• ICT Logs</li> <li>• Marketing datasets (e.g. email lists).</li> <li>• Images, video and other media assets (unstructured data).</li> <li>• CRM Data</li> </ul>

Host/custodian	The organisation or group responsible for looking after a data set in the long term/ including ensuring it is accessible/ secure/ and up to date
Metadata	A description of a dataset with details such as how the dataset was collected/ by whom/ its quality/ and access restrictions.
Publish	To make data available for visualisation or download via the internet
Web service	A web service is a method of communication between two electronic devices over a network. It is a software function provided at a network address over the web, with the service always-on, similar to the concept of utility computing. Web services are designed to support interoperable machine-to-machine interaction over a network. They typically use standard web protocols such as HTTP or HTTPS and can provide data in formats like XML and JSON

#### 4. RISK CATEGORY

This policy covers the following risk categories.

Strategic	Governance	Service Delivery	Reputational	Financial	Operational	People
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

#### 5. RELEVANT DOCUMENTATION

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

##### Primary Policy

[Information and Communications Technology \(ICT\) policy.pdf](#)

##### Relevant documentation

###### Internal

[Risk management policy](#)

[Information Technology Policy](#)

[Intellectual Property Management Policy](#)

[FRDC Privacy Policy](#)

[Records Management Policy](#)

[Information Management Policy](#)

[Risk register](#)

[Data breach procedure](#)

<a href="#">Data management policy</a>
<a href="#">Data request procedure</a>
<b>External</b>
<a href="#">NFF Farm Data Code</a>
<a href="#">ISO8000 Data Quality Standard</a>
<a href="#">ISO27001 Data Security Standard</a>

## 6. TRAINING

The training for the procedure will be delivered/undertaken by the following method:

- Procedure to be emailed to all staff when signed

## 7. PUBLICATION

This procedure is to be made available on the FRDC website.

This procedure is to be made available on the directors' site.

## 8. ACTIONS

The Data Governance Framework (Attachment 1) outlines the data management steps the organisation undertakes

## 9. ATTACHMENTS

#	Description
1	FRDC Data Governance Framework
2	FRDC Data Governance Framework – on a page

# Attachment 1 FRDC Data Governance Framework

## PURPOSE

The purpose of the FRDC data governance framework is to:

1. Establish the **principles, guidelines and best practices** for the **effective management** and use of data within FRDC.
2. Align the policies and procedures to ensure that FRDC data is **secure, accessible and reliable** within a clear system of controls.
3. Define the **roles and responsibilities** for stewardship of FRDC data and the information systems that support the framework.
4. Ensure that FRDC decision making, planning and reporting is informed by **secure, well managed, high-quality data** and that data that is presented to stakeholders is secure and accurate and is accompanied with appropriate data agreements, metadata and other supporting materials to ensure quality and trust.
5. Define how data governance will be **monitored and reviewed** within FRDC
6. Provide recommendations for the **tools, policies and techniques** that should/will be adopted by FRDC to effectively and securely manage data while ensuring data quality.

To manage and control FRDC data risks, data is considered and described as part of five stage Data Lifecycle (see diagram below), enabling creation of a well governed, trusted FRDC data environment.



- 1. Collection** The creation, acquisition or capture of data.
- 2. Access** Ensuring that data is secured and only authorised users have access to necessary data.
- 3. Storage** The appropriate retention and organisation of data.
- 4. Use** The appropriate utilisation of data by the appropriate authorised users.
- 5. Archive and Disposal** The ongoing storage of data in use or deletion of data that is no longer required.

## DOCUMENT MANAGEMENT

It is recommended that the framework is reviewed every 12 months to ensure that it is responsive to employee and partner feedback, is aligned with current legal requirements and that all controls remain relevant to capturing all data risks that are in what is a very fast changing environment.

## GENERAL

### *Overview*

The FRDC data governance framework (the framework) contains the information needed to maintain a consistent, managed approach to the control of FRDC data. This is required to mitigate data management and quality risks and to ensure efficient use of data across all FRDC operations and projects.

High quality, well managed data provides the foundation for FRDC decision making. It reduces risks and inefficiencies and enables high quality outputs across project and business as usual activities. A consistent governed approach to data management is also key to developing trust, as it enables new opportunities to use data to optimise industry social licence, productivity, markets and products.

This framework has been designed to be used as a reference. It can be referred to when managing data when planning or executing projects or when using data to help minimise risk to FRDC and other stakeholders. The framework has been carefully designed to ensure that it does not add unnecessary overhead impeding the use of data but rather, as much as possible leverages existing policies, tools and services already in use at FRDC as much as possible.

## Principles

The data governance principles define the rules against which all data in use at FRDC should be considered. FRDC subscribes to the following data governance principles:

### FRDC Data Governance Principles

1. **Transparent, clear and honest collection, use and sharing data** FRDC will be able to clearly communicate to relevant interested parties the purpose/s for which data is being collected, used and shared
2. **Fair and equitable use of data** Recognise that contributors should benefit from FRDC use of their contributed data where agreements are in place.
3. **Ability to control and access data** Only use data for the purposes specified in the terms agreed by the contributors (including licences etc)
4. **Documentation and record keeping** ensure that all processes and decision making related to data are documented in a clear and comprehensive manner
5. **Portability of data** Provide contributors with the ability to retrieve their data
6. **Keeping data secure** Take all reasonable and prudent steps, data is protected at all times from unauthorised access, alteration, damage or destruction
7. **Compliance with National and International Laws** promptly notify any Contributor whose identifying information will be (or has been – if prior warning is not possible) disclosed.

The principles extend those that were originally developed for the NFF Farm Data Code. The principles have been tailored to align with the FRDC ICT & Digitalisation Strategy. They form the foundation for how FRDC thinks about data.

### **PRINCIPLE 1. Transparent, clear and honest collection, use and sharing of data**

FRDC will ensure that procedures are in place that enable clear communication with stakeholders about what data is collected by FRDC and will encourage project providers do the same. It is expected that partner organisations have established data governance and management procedures in place that FRDC can refer to when communicating with stakeholders. As a result, FRDC will be able to clearly communicate to relevant interested parties the purpose/s for which data is being collected, used and shared (including the use and sharing of Aggregated Contributor Data<sup>1</sup>).

In order to achieve this, FRDC data sharing agreement will adhere to best practice considerations below, and will encourage researchers and providers must be able to provide data contributors/stakeholders with plain-English information detailing:

---

<sup>1</sup> <https://toolkit.data.gov.au/data-integration/data-integration-projects/part-4.html>



### Best Practice Data Sharing Agreement considerations

- The identity of contracting party/ies, and any affiliates who may receive project/industry data pursuant to the contract;
- What data will be collected about them and their organisation;
- How that data will be used and managed;
- The processes and conditions for data retrieval and service termination; and,
- Any risks or detriments that may adversely affect contributors who share data with the FRDC funded project.
- Provide appropriate updates about any changes to this framework, policies, procedures and contracts and where a change to terms and conditions is proposed, obtain consent or provide an avenue for the data provider to reject the change without incurring a financial penalty or loss.
- Provide mechanisms for data contributors to enquire about the collection, use, storage, security and sharing of their data.
- Notify contributors of the legal jurisdiction in which their data is stored.
- Notify contributors of any breach or compromise to the security of the data stored about them.

### *PRINCIPLE 2. Fair and equitable use of data*

FRDC will:

- Only collect, use and share data for the purposes that have been made clear in the terms with the contributor.
- Recognise that contributors should benefit from FRDC use of their contributed data where agreements are in place.
- Ensure that the privacy of contributors is appropriately protected (see FRDC privacy policy and ISO 8000 requirements) and that data is collected, stored and used in alignment with the FRDC data lifecycle
- Ensure data retention is in line with Records Management Policy

### *PRINCIPLE 3. Ability to control and access data*

FRDC will:

- Only use data for the purposes specified in the terms agreed by the contributors (including licences etc). The FRDC standard data sharing agreement can be found under the Agreement Template library
- Preserve the ability of the contributors to determine who can access and use all or part of their contributed data held as a government record (i.e. title, organisation undertaking the project etc) where possible
- Protect sensitive data, such as personal/financial information, confidential information or intellectual property (in alignment with the data classification process described in the data lifecycle).

- Comply with obligations imposed by the Privacy Act 1988 (Cth), including the Australian Privacy Principles.

#### ***PRINCIPLE 4. Documentation and Record Keeping***

FRDC will

- have a record keeping system in place (data request register and data catalogue) to ensure that all processes and decision making related to data are documented in a clear and comprehensive manner.

#### ***PRINCIPLE 5. Portability of Data***

FRDC will:

- Provide contributors with the ability to retrieve their data – in both a processed (cleaned) and unprocessed form – for storage and/ or use in third party systems (this includes during any agreed Data Retention Period). See the FRDC records management policy for more detail on the FRDCs standard enduring data retention period.
- At the request of a contributor, delete any data (commercial, public or private) relating to that contributor unless required for government record as a condition of funding (as determined/agreed in the funding agreement).

#### ***PRINCIPLE 6. Keeping Data Secure***

FRDC will:

- Take all reasonable and prudent steps, in line with the Information Management Policy and licence terms to ensure Commercial Data, Private Data and Public Data are protected at all times from unauthorised access, alteration, damage or destruction.
- Promptly notify a contributor where an attempt (successful or otherwise) has been made to gain unauthorised access to, or damage or destroy their Public Data or Private Data in alignment with the FRDC Data Breach Procedure.
- Implement a backup and recovery regime that is appropriate for the scale, sensitivity and timeliness of the contributed Data in alignment with the FRDC Data Backup Procedure.
- Ensure all staff and subcontractors are trained to comply with the terms of this framework as part of the ICT section of the staff induction.

#### ***PRINCIPLE 7. Compliance with National and International Laws***

Where FRDC are required by law to provide data to a third party, FRDC will:

- Avoid disclosing any Commercial Data or Private Data as per obligations under the *Privacy Act 1988*; or,
- If Commercial Data or Private Data must be disclosed, where legally permissible FRDC must promptly notify any Contributor whose identifying information will be (or has been – if prior warning is not possible) disclosed. Note business confidential is not subject to FOI.

## Roles & Responsibilities

- Chief Data Officer/ Chief Information Officer
- Data Steward
- Data Provider
- Data User

These roles can be mapped directly to existing FRDC roles and to project stakeholders.

### **DATA GOVERNANCE ROLE 1. Chief Data Officer**

The Chief Data Officer (CDO) is responsible for the management and maintenance of the contents of this framework including how it is operationalised across the RDC. While the FRDC Board is accountable for ensuring effective organisational governance (and the GM – Business responsible for the Data Breach procedure), the CDO is responsible for ensuring the organisation aligns to defined policy and undertakes the appropriate management of data disputes and importantly data breaches to policy. FRDC's Chief Data Officer is the General Manager ICT & Digitalisation

The CDO:

- works in partnership with FRDC Data Stewards to ensure that FRDC ICT & Digitalisation controls are implemented, effective and fit for purpose.
- monitors data use across the RDC to ensure compliance and looks for opportunities to link and analyse datasets to provide corporate, research and industry value.
- designing and implementing a test plan(s) to demonstrate that the policies, procedures and systems that are in place adequately mitigate all risks associated with the datasets for which they are responsible (and ensuring the currency of the risk assessment for the dataset).

### **DATA GOVERNANCE ROLE 2 Data Steward**

Data Stewards are usually systems owners who take ownership of FRDC data through their business as usual project or administrative activities.

FRDC Data stewards are responsible for:

- Implementing, monitoring, maintaining and enhancing when required, the policies and procedures defined by FRDC that ensure effective day-to-day management and quality of FRDC data. This includes all aspects of collection, storage, processing, transmission, ownership, sharing and security of data to internal and external systems and stakeholders.
- Understanding the data requirements of their system or project.
- Having clarity of the data they own and for which they are responsible.
- Ensuring that the policies, principles and procedures outlined in the framework are implemented across the Data Lifecycle for the data for which they are responsible.
- Ensuring that the required monitoring and review processes are undertaken across all datasets under their management within the defined periods.

- establishing data-quality metrics, metadata<sup>2</sup> and requirements for the data sets under their stewardship, including defining the values, ranges, and parameters that are acceptable for each data set (the data specification).
- Seeking approval from the GM Business & Finance prior to the disposal of any data under their management when it is no longer required and ensuring that personal data is disposed of in alignment with the requirements of the FRDC Records Management Policy.
- Highlighting risks associated with the data for which they are responsible and working with the CDO to ensure all risks are effectively mitigated.

Systems Owners fulfil the role of data stewards within the FRDC. However, the General Manager – Finance & Business is responsible for ensuring that Agreements templates are compliant with the framework.

### ***DATA GOVERNANCE ROLE 3 Data Provider***

In addition to FRDC data management roles, the framework also identifies/recognises the role of the Data Provider.

Data Providers include stakeholders that provide data to FRDC. They provide the raw data that:

- Enables corporate business as usual functions and reporting,
- Provides input into and outcomes from research projects,
- Enables market reporting and intelligence,
- Supports industry programs and,
- Enables and optimises marketing, extension and adoption activities

The framework seeks to build trust with Data Providers by ensuring they have visibility and control over their raw data and that their privacy and confidential information is protected. This is achieved through the holistic application of all aspects of the Data Governance Framework, clear communication and effective use of data agreements.

### ***DATA GOVERNANCE ROLE 4 Data Users***

All FRDC employees, stakeholders, partners, research providers, Government departments, and the general public may be users of FRDC data, and hence, they can be impacted by the data held, directly or indirectly.

All FRDC employees (and contractors) are responsible for identifying risks related to the data being accessed and used in all business as usual activities and escalating any data anomalies, risks, security issues or data quality concerns to the responsible Data Steward.

All Data users need to be identified (usually by the Data Stewards) and included and consulted in data-related decisions that impact FRDC, Industry or their individual businesses. Data users will be instrumental in designing and agreeing all data access agreements and working with Data

---

<sup>2</sup> ARDC Guide to MetaData: <https://ardc.edu.au/resource/metadata/>

Stewards to ensure all elements of interaction, access, quality and management are agreed and managed.

Ultimately Data Stewards will partner with Data Users to ensure they:

- Understand the importance of a dataset and its impacts.
- Are collaborative and engaged.
- Are a champion in their data and area of expertise.

## Managing Data



To support the effective management of data, FRDC have created a Data Catalogue to manage and monitor all data within the organisation and linked third party managed data of interest to the organisation. The data catalogue supports the capture of metadata.

### **DATA MANAGEMENT ASPECT 1 Data Collection**

Data is collected across FRDC to support corporate, research and Industry outcomes. Collecting data in a structured, governed way is essential to ensuring data quality. The collection of data must be consented to by the Data Owner and a Data Steward must be assigned by the Chief Data Officer to each new dataset being collected and stored by FRDC.

Before data is collected appropriate planning must take place. The data should be classified against the framework classification guidelines (see the following section for data classification guidance). Storage options will be governed by the Information Management Policy

The ability to reuse existing datasets or link the dataset to existing datasets must be considered. As such are any pre-existing data standards or protocols in place within the scope of the data that should be sought out, considered and adhered to. If not, the Data Steward should seek the opportunity to develop, document and communicate a new data specification across FRDC and/or Industry (see Data Steward Role Description in the previous section).

The importance and benefits of the data collected must justify the cost of collection. Cost considerations should include the development, procurement and ongoing maintenance of the data collected. From an FRDC perspective, this cost relates to the resources used in supplying, collecting, processing, storing and using the information within a dataset.

### **DATA MANAGEMENT ASPECT 2 Data Quality**

Ensuring data is fit for its intended purpose by focusing on completeness, accuracy, consistency and timeliness of data is essential. The framework aims to support Data Stewards and FRDC staff and Contractors to monitor and manage the quality of the datasets under their stewardship by requiring the following:

Control	Description
Accuracy	<ul style="list-style-type: none"> <li>• Data should be sufficiently accurate for its intended purposes.</li> <li>• Data should be captured on the principle of 'getting it right first time', so captured once, captured as close to the point of activity as possible, with clear and simple actions and only limited, if any, manual intervention (e.g., administration, data cleansing)</li> <li>• Accuracy is likely to be higher if employees, contractors and research</li> </ul>

	<p>partners who provide data are aware of its importance and quickly have access to information based upon it, especially if they obtain some benefit for their effort in securing the quality of that data</p> <ul style="list-style-type: none"> <li>• Accuracy is a balance between the importance of data and the cost of collection. Where there are compromises on accuracy for the sake of cost, the limitations of data should be made clear to Data Users. Compromise is unlikely to be appropriate in the case of corporate financial information or other legislated outcomes.</li> </ul>
Completeness	Identification and highlighting missing, incomplete or invalid records can provide an indication of data quality and highlight ways in which the data capture process can be improved.
Consistency	Data should be collected using stable and consistent data collection processes, or where changes or differences are necessary, sufficiently documented, monitored and understood so information produced is stable and consistent.
Timeliness	Data should be captured as quickly as possible after creation and must be available for its intended use within any agreed time period (often defined in the data sharing agreement).
Fitness for use	Data should be collected, stored and used consistently, in compliance with relevant business, industry or government requirements, rules or definitions.
Monitoring and Audit	Data controls should be monitored and logged to enable review and auditing of data quality so that issues can be highlighted as quickly as possible to Data Users.

### **DATA MANAGEMENT ASPECT 3 Data Classification**

The table below outlines the 5 types of data classification applied within the framework. All FRDC data can be classified under one of the levels. Levels 2-5 are confidential information and require specific controls and consideration. The higher the level, the greater the required protection.

Level	Description	Examples
1	<b>Public Information.</b> Data that if breached owing to accidental or malicious activity would have an insignificant impact on FRDC. Equivalent to FRDC Intellectual Property Category A.	Published research data, published information about FRDC, Annual Reports, Strategic Plans, Terms of Reference etc.
2	<b>Private.</b> Information that may contain some sensitivities, with publication to be on the	Unpublished IP, Business unit documents, process and procedures.

	basis of approval by data contributors on a case by case basis. Equivalent to FRDC Intellectual Property Category B.	
3	<b>Sensitive.</b> Information that would cause risk of material harm to individuals or FRDC if disclosed. Equivalent to FRDC Intellectual Property Category C.	FRDC Financial Information, Employee (including contractor) Information, Industry or supply chain personal information, unpublished industry data, unpublished research data (including personal information), customer (and other personal) data (including surveys etc).

### Data Classification Process

Data Stewards are required to determine the data classification of the data sets for which they have responsibility. This assessment should be reviewed periodically. The data classification assessment will determine how the framework and supporting policies apply to the new data set. Data stored in FRDC ICT systems such as CRM, SharePoint etc. will provide many of the controls required to manage the data within classification requirements. Special consideration will be required for data created by newly deployed systems and data held outside of FRDC ICT managed repositories.

#### Data classification process for FRDC data:

The following are the minimum six steps required to complete the data classification process for FRDC data:

#### 1. Identify and confirm the Data Steward

The CDO or the Principal Investigator should ensure a Data Steward has been identified to a dataset. The data should be classified by the Data Steward at the earliest possible opportunity.

#### 2. Assess data risks

Use the Data Risk Assessment Template <sup>3</sup> to record the risks associated with the dataset.

#### 3. Apply the classification to the data

The highest classification level determined by the risk/impact assessment must be applied to that Information Asset.

#### 4. Apply controls

<sup>3</sup> Data Risk Assessment Template: <https://toolkit.data.gov.au/data-integration/risk/risk-assessment-guidelines.html>



Work in conjunction with the FRDC ICT Manager to ensure that all data controls are in place, for example access control, back up etc. Additionally ensure that the data is placed under review by the FRDC ICT by registering it within the data catalogue.

## **5. Audit logs**

An audit process must be put in place for each data set to ensure it is capable of providing a 'trail of evidence' which can be used to investigate inappropriate or illegal access. FRDC ICT will ensure that audit log access controls are in place with explicit user authentication needed to view the audit log. For systems such as SharePoint, these audit logs have already been established by the FRDC ICT team, for additional systems not already under ICT management audit logs must be considered.

## **6. Disposal of data**

When the data is no longer required. The data should be disposed of in accordance to the guidelines described in the Data Disposal section of the framework.

Once the data has been classified the classification is to be logged as metadata in the data catalogue. The data catalogue also records any additional relevant information to ensure required controls are in place and documented for future audit.

### ***DATA MANAGEMENT ASPECT 4 Data Access***

Data access/sharing may be initiated by a Data Steward; however, it is generally initiated by a request to a Data Steward for data. Requests would usually come from an FRDC business unit, Industry, Government or a research partner.

A request for Data Access should describe the purpose for which the data will be used to aid the Data Steward assess the need for the development of a Data Sharing Agreement. The requests for use will also enable the Data Steward to capture all use cases of a data set in the FRDC Data Request Register.

Data Stewards should seek the following information regarding the use of data under their stewardship:

- Is the use of data in line with the purpose for which it was collected and why it is required?
- Is the requested data suitable to satisfy the request and will access provide corporate or industry benefit? The Data Steward will have the best understanding of what can and cannot be achieved with the dataset.
- Can the dataset be shared legally? Is there a data sharing agreement in place with the requesting party (see the following section for further information regarding data agreements)? Have legal and ethical considerations been considered? Are there any sensitivities to the data that need to be considered?
- The duration the user needs the data, and the expected outputs and outcomes.
- Are there any licences associated with the data, if so, what are the terms? Are there any restrictions to the use of the data? It could also be the case that the licence mandates

that the data only be used for certain purposes or that the rights to any derived data are passed to the licensee.

As with the collection of data the costs of providing access to data should be considered. It is likely that additional services and support will be required to enable and maintain the shared data. All the information sought from asking the questions above should be stored in the FRDC data catalogue for future reference and audit.

#### Assessing a data request checklist

- What, if any, process for authorisation is required for the Data User to access the dataset? Who facilitates this process? How long will any authorisation be valid? Are controls in place, can controls be put in place?
- Will a legally binding data access agreement be needed to govern the access and use? Who needs to complete this undertaking or agreement?
- Are there any licences associated with the use of the data? Does FRDC need to agree to any licence terms ahead of the data being used?
- Does the Data User need to meet any specific criteria to access the data?
- Does the Data User have a history of good data handling practices? Does the user need to seek endorsement of their data management practices from an enabled manager in their organisation?
- Does the Data User need to be trained in safe use, data storage and technical skills? Who will provide the training?
- What conditions (legal and non-legal) need to be in place to control the misuse of data? Are these clear to the Data User?
- Are there any restrictions on who may apply to access the data (e.g. must be an Australian citizen, employee or researcher of a university etc)?

#### **DATA MANAGEMENT ASPECT 5 Data Sharing**

FRDC staff should use the standard agreements provided by FRDC. Data sharing agreements are made between a Data Provider and FRDC or between FRDC and a Third Party organisation who is receiving a dataset for use (for example, a solution provider, research institution, government department, Industry organisation etc).

These agreements must include the purpose for which the data will be used. Any agreement must also specify what the data can and cannot be used for. In addition to the specifics of use, the data sharing agreement should also define all expectations regarding the format in which the data should be shared including any specifications, protocols and standards etc.

Datasets that are created during the delivery of research projects that are delivered under the Standard FRDC Project Agreement ensure that the required restrictions and affordances are included to clearly articulate any limitations for onward use.

A data sharing agreement or data licence agreement is the means of ensuring all aspects of the data sharing, the participants and their responsibilities are documented. It is best practice to make data sharing/licence agreements available publicly on the FRDC website to ensure transparency.

### **DATA MANAGEMENT ASPECT 6 Data Storage**

The storage needs of each dataset needs to be considered. Data may be stored as it is collected, processed, shared as well as when it is archived (including by 3rd party systems when cloud services are used).

Data Storage is as advised in FRDC's Information Management Policy.

#### **Data Storage Checklist**

1. From what physical location(s) will the data be accessed?
2. Does there need to be auditing/checks of these locations?
3. What physical supervision is appropriate?
4. What ICT security needs to be in place? Will the security classification of the data influence ICT security requirements?
5. What electronic supervision as well as auditing/recording of use is available?
6. Is certification of physical and/or ICT environment necessary? If so, by whom?
7. Do the controls limit misuse (by mistake and deliberate), interference, unauthorised access, modification, loss or disclosure?
8. Do users understand how to access the data safely in the ICT and/or physical environment? Is training required?
9. How will data transfer into and out of a secure environment be managed?

### **DATA MANAGEMENT ASPECT 7 Data Security**

Data should be secured in alignment with the relevant ICT Security Policies.

**Data security requirements should be reviewed every twelve months by CDO** to ensure compliance. In addition to any existing security measures the classification of the data should also be reviewed and that the privacy requirements are in line with those detailed in the FRDC Privacy Policy.

### **DATA MANAGEMENT ASPECT 8 Data Use**

Data must be used for the purposes for which it is collected or within the terms of the associated data sharing agreement or licence. It is the responsibility of the Data Steward to ensure that all parties with access to the datasets (including all employees, contractors and research partners) under their stewardship are using the data appropriately.

Personal data should be given additional consideration and only be used as per the guidance described in the FRDC Privacy Policy.

Datasets that are augmented - including cleansing, de-identification, summarising, linking or re-encoding must be captured in the data catalogue by the Data Steward and registered as derivative of the original datasets.

Data Use Considerations:

- Does there need to be any animal or human ethics approval from a governance body that considers the ethics of the data use?

- Are there any restrictions (e.g. legal or data provider/data steward imposed restrictions) on how the shared data may be used?
- Is consent from the original data providers required?
- Is the classification of the data in alignment with the intended use?

#### ***DATA MANAGEMENT ASPECT 9 Data Disposal***

Data must remain available, accessible, retrievable and usable for as long as a business need exists, a research report is published, or as long as legislative requirement, licence or Industry policy require them to be kept.

Disposal should be in line with the FRDC Records Management Policy

## What does successful Data Governance look like?

### Best practice data governance

Through the ongoing application of the Data Governance framework, FRDC will measure success through achieving the following outcomes:

- Data roles and responsibilities are well known and understood by new and existing FRDC employees and contractors.
- Tools and services are in place to support the data management lifecycle.
- There is ongoing monitoring and identification of risks, mitigated with controls to prevent data breach and build industry trust.
- High quality data is stored by FRDC enabling robust decision making and requiring minimal remediation.
- Data sets are easy to find and use by FRDC staff and contractors avoiding duplication of effort, inconsistency and inefficient use of industry resources.
- The provenance (history) of data held by FRDC is known and can be demonstrated with minimal operational effort.
- Robust and where possible, automated review processes are in place to monitor and maintain compliance of FRDC data against this framework and associated policies.
- Specifications and standards are defined and in use enabling data interoperability across FRDC business units, stakeholders, partners, and research providers.
- Data is stored and managed securely by FRDC and its partners in alignment with broader FRDC ICT and cyber security policies ensuring authentication and access control of data with appropriate audit history.

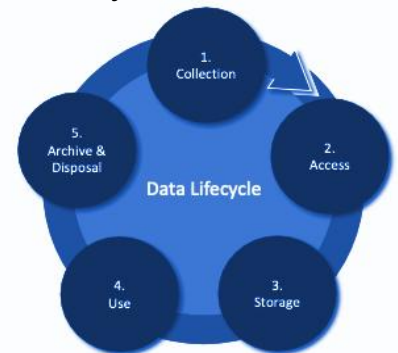
The data governance framework is dependent on the clear assignment of roles and their associated responsibilities across the data lifecycle from collection through to disposal.

## Attachment 2 Data Governance on a Page

FRDC strives to apply best practice data governance to all aspects of the data lifecycle

FRDC adheres to the following governance principles

- 1. *Transparent, clear and honest collection, use and sharing data***
- 2. *Fair and equitable use of data***
- 3. *Ability to control and access data***
- 4. *Documentation and record keeping***
- 5. *Portability of data***
- 6. *Keeping data secure***
- 7. *Compliance with National and International Laws***



### Best practice data governance -snapshot

- Data roles and responsibilities are well known and understood by FRDC employees and contractors.
- Tools and services are in place to support the data management lifecycle.
- Ongoing monitoring and identification of risks, mitigated with controls to prevent data and build trust
- High quality data is stored by FRDC enabling robust decision making and requiring minimal remediation.
- Data sets easy to find and use, avoiding inconsistency and inefficient use of industry resources.
- Specifications and standards are defined and in use enabling data interoperability across FRDC business units, stakeholders, partners, and research providers.
- Robust and automated review processes to monitor and ensure compliance with data governance framework

The following outputs underpin FRDC's Data Governance Framework

- **Secure system** aligned to FRDC's Information Technology Policy
- **FRDC Data Catalogue** detailing FRDC derived & R&D investment derived data assets
- **FRDC Data Request Procedure** underpinned by Assessing a data request checklist
- **FRDC Data Request Register** for transparency and good record keeping
- **FRDC Data Sharing Agreement template** with plain English summary of data use
- **FRDC Data risk register** detailing data classification process & risk controls for FRDC data
- **Data retention guidance** in line with Records Management Policy






# Data Management (Governance) Procedure

Final Audit Report

2025-04-02

Created:	2025-04-02
By:	nicole stubing (Nicole.Stubing@frdc.com.au)
Status:	Signed
Transaction ID:	CBJCHBCAABAAek22Oc32yFZr_iSa-qD8pUHrBVlKWg1J

## "Data Management (Governance) Procedure" History

-  Document created by nicole stubing (Nicole.Stubing@frdc.com.au)  
2025-04-02 - 4:47:16 AM GMT- IP address: 27.33.210.30
-  Document emailed to Kyaw Kyaw Soe Hlaing (kyawkyaw.soehlaing@frdc.com.au) for signature  
2025-04-02 - 4:47:35 AM GMT
-  Email viewed by Kyaw Kyaw Soe Hlaing (kyawkyaw.soehlaing@frdc.com.au)  
2025-04-02 - 5:00:34 AM GMT- IP address: 104.47.71.254
-  Document e-signed by Kyaw Kyaw Soe Hlaing (kyawkyaw.soehlaing@frdc.com.au)  
Signature Date: 2025-04-02 - 5:01:10 AM GMT - Time Source: server- IP address: 220.233.142.2
-  Agreement completed.  
2025-04-02 - 5:01:10 AM GMT



Adobe Acrobat Sign