Research Data Management Procedure

Section 1 - Purpose

(1) This Procedure documents the expected practices for research data management, including data collection, storage, use, sharing, retention, and offboarding activities.

(2) This Procedure should be read in conjunction with the Research Data Management Policy to assist Researchers to understand and apply the principles of the Macquarie University Code for the Responsible Conduct of Research (Macquarie Research Code) to the management of Research Data.

Scope

(3) This Procedure applies to anyone who conducts Research or research support under the auspices of Macquarie University, as per the Macquarie Research Code.

(4) Researchers may consult with a Research Data Steward at any time for advice in relation to this Procedure.

Section 2 - Policy

(5) Refer to the Research Data Management Policy.

Section 3 - Procedures

Data Governance

(6) Researchers should acknowledge and clearly specify details regarding ownership (refer to the Research Data Management Policy for the default arrangements), custodianship, access, licensing, retention, and intended dissemination and use of any data collected, generated, or collated as part of their research, including:

a. when Data are obtained from external databases, restricted access databases, or via contractual arrangements, the location of the original data, applicable Licenses, or key information regarding the database (such as conditions of use and retention) from which it will be obtained, should be reported, along with relevant contractual details;
b. when Data is intended to be produced collaboratively with researchers outside of Macquarie University, the Research Collaboration with Third Parties Procedure should be followed with regard to the establishment of a Research Collaboration Agreement or an alternative research third party arrangement; and
c. Research that involves Indigenous Data needs to consider Indigenous Data Governance, the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) Code of Ethics for Aboriginal and Torres Strait Islander Research, Indigenous Cultural and Intellectual Property (ICIP) principles (e.g. True Tracks Principles) and Maiam nayri Wingara Indigenous Data Sovereignty principles in the development of a research data agreement with the peoples or Communities.

Data Management Planning

(7) All Researchers must clearly establish their intentions related to each stage of the Data Lifecycle for Data associated with their project, prior to project commencement as follows:

a. a Data Management Plan (DMP) must be developed for all projects (and lodged online for certain project types per clause 7(b)). It is expected that this plan encompasses regulatory approval, data governance, and data management across all stages of the Data Lifecycle, including appropriate end-of-project plans (retention, dissemination, and archiving) so that other researchers (or the researchers themselves in the future) may benefit from the Data. Planning should incorporate, to the extent possible, the Findable, Accessible, Interoperable, and Reusable (FAIR) and Collective benefits, Authority to control, Responsibility, and Ethics (CARE) Data Principles.

b. A Data Management Plan (DMP) must be registered and updated as appropriate, either annually or as changes arise (for example when Researchers change institutions or withdraw from a collaborative project, or when the program of research, funding source or objectives are changed) in the Forms for Research Applications (FoRA) system by the Principal Investigator of the project, a delegated research data custodian, or the Graduate Research student for all projects which are:

   i. seeking Human Ethics approval through a Macquarie University Human Research Ethics Committee (HREC) (following the requirements of the National Statement on Ethical Conduct in Human Research 2025);

   ii. seeking Animal Ethics approval through the Macquarie University Animal Ethics Committee (following the requirements of the Animal Research Act 1985 and the Australian Code for the Care and Use of Animals for Scientific Purposes 2013 updated 2021);

   iii. successful in gaining funding from the Australian Research Council (ARC) and/or the National Health and Medical Research Council (NHMRC);

   iv. involving Researchers accessing Sensitive or Highly Sensitive Information (following the Research Data Sensitivity, Security and Storage Guideline). This includes information which is under regulatory control (such as that involving controlled technology per the Defence Trade Controls Act 2012) or information associated with projects that are under regulatory control, for example from national security legislative or governance instruments such as the Defence Security Principles Framework;

   v. being undertaken by a Graduate Research student at Macquarie University;

   vi. successful in gaining funding from other Category 1-4 grants (following the Australian Government Specifications for Categories of Research); or

   vii. successful in gaining internal Macquarie University funding.

      - Note that the requirement of clause 7(b) to register a Data Management Plan (DMP) online will be progressively released to these various cohorts from 2021.

c. Any proposed variations to the DMP of a project that has already gained Human Ethics approval must be requested following the standard processes for an amendment. It is the responsibility of the Principal Investigator to ensure that appropriate approval is obtained for all amendments prior to implementation.

Data Storage, Retention or Disposal

(8) Data should be stored on and backed up to data infrastructure sanctioned by Macquarie University. Refer to the Research Data Sensitivity, Security and Storage Guideline for help in assessing the sensitivity of Data, appropriate security measures, data resilience and retrieval requirements and suggested platforms.

(9) The significance of Research Data is not always immediately apparent and permanent retention should be considered the default. Permanent retention of data through deposit of Data Outputs into a discipline-specific repository, trusted Data Repository or the Macquarie University Research Data Repository as appropriate is best

practice for all projects. Data Retention is required where the Data, Primary Materials, and records are crucial to the substantiation of the research findings, cannot be readily or practically duplicated, and the Research is:

a. controversial or of high public interest, or has influence in the research domain;
b. costly or impossible to reproduce or substitute if the Primary Data is not available (i.e. cannot be substituted with an alternative dataset of acceptable quality and usability, or if data reproduction would place unnecessary burden on human research participants or animals); or
c. relates to the use of an innovative technique for the first time.

(10) If Data is not or cannot be retained permanently, the reason for its disposal should be explained in the DMP, and its disposal protocol should be articulated. Data not retained permanently should be archived:

a. in Macquarie University infrastructure or appropriate alternative archival storage that meets the data’s privacy, security, legal and sensitivity requirements;
b. to demonstrate the outcomes of any Research and to provide defence of any event or any challenges. Sufficient records, materials and Data must be retained for a specific period following the completion or closure of project. Publicly available third-party data, such as legal materials, articles, reports, and various forms of secondary literature or owned by other researchers or organisations, may not necessitate retention. However, data sources must be documented and retained.
c. for a minimum period specified by prevailing standards for the specific type of research and any applicable state, territory or national legislation. For example, per State Archives and Records Authority of New South Wales General Retention and Disposal Authority: GA-47, Research Data not of major significance but with potential long-term impact (including, but not limited to, environmental data, or health data such as research involving psychological testing or medical research involving children) must be retained for a minimum of fifteen (15) years after completion of research activity or until subject reaches or would have reached the age of twenty-five (25) years. Other Research Data must be retained for a minimum of five (5) years from the completion of the project or from the time that the results of the research are disseminated.
    i. Once the duration of Data Retention, which is necessary to fulfil legal, regulatory, institutional, and research requirements, has expired, and the Data is no longer required for ongoing research, compliance, or reference, it should be securely, appropriately, and permanently deleted.

(11) When a Researcher leaves Macquarie University, where possible, the original Research Data and materials (and, where appropriate, other relevant information or documentation) are retained on Macquarie University's infrastructure to meet State Records NSW legislation. The Researcher must arrange and record new 'data custodian', 'data storage location' and Data Access Condition in Data Management Plan (DMP).

(12) When disposal is justified, data used in research should be disposed of in a manner that is safe and secure, consistent with any consent obtained. It should follow the National Statement on Ethical Conduct in Human Research 2025 and any legal requirements and as appropriate for the design of the research.

(13) In the event that research results are challenged, all associated records, materials and data must be retained unaltered until the matter is resolved. Research records that are subject to allegations of a Breach of the Macquarie Research Code or are subject to legal proceedings must not be destroyed or altered. Platforms used to store data must have appropriate security and audit capabilities attesting to the integrity of the Data.

Metadata and Data Dissemination/Publication

(14) Metadata should be captured for all data collected, generated, or by researchers.

(15) At the conclusion of a project, or at the time of publication or dissemination of a Research Output, researchers should also disseminate their data as a Data Output, following best practice in their discipline and in accordance with

any publisher or funder requirements.

(16) Data Outputs should conform to the FAIR Data Principles as far as possible and any relevant discipline-specific Metadata guidelines or practices and consider CARE Principles if research involves or is related to Indigenous peoples or communities. Appropriate context (descriptive, technical, methodological, and access information) should be provided, either within the Data or in a separate Metadata record for the Data.

(17) Data should be disseminated, regardless of whether the Data directly supports the research findings. Data can be disseminated openly to the public or through restricted or Mediated Access to meet ethical, contractual or Intellectual Property requirements. Such data should be as comprehensive and open as possible, and as closed as necessary (cf. EU Horizon 2020). Any request not to disseminate data must be justified.

(18) Sensitive data can and should be disseminated with appropriate safeguards. Researchers must determine and apply appropriate techniques for safely disseminating Research Data which includes sensitive information. This can involve creating De-Identified or Anonymised Data by removing or aggregating sensitive information from the Data, or by controlling access to a Data Output (or some combination of these approaches). Note that by combining data sources, it is growing ever more possible to re-identify data, so de-identification strategies must be carefully considered and explained.

(19) Data that is being disseminated (a 'Data Output'):

a. must be deposited in a trusted Data Repository including discipline-specific, general-purpose, or Macquarie University Research Data Repository, or in national or international database, registry, or collections, as per good practice in the discipline and in accordance with any publisher or funder requirements. Dataset-level Metadata should be deposited in the Macquarie University Research Data Repository if Data is published elsewhere (including a link to the Data);
b. must have a License assigned to it providing clear parameters around the reuse of the Data Output:
    i. An open license, such as a Creative Commons Attribution 4.0 International (CC BY 4.0) or comparable Open Data Commons license, is the default for all general data produced by Researchers at Macquarie University.
    ii. Data requiring Mediated Access (i.e., restricted or special access often applied to Sensitive or Highly Sensitive Data that users may not redistribute) should use a repository specific license, for example, Macquarie University Standard License Terms and Conditions of Use, which allows use of Data with attribution but prohibits redistribution of that Data. Data may be licensed more restrictively upon request and with appropriate justification (refer to Research Data Sensitivity, Security and Storage Guideline, clause 34(b)); and
c. must have a Persistent Identifier (PID) assigned to the dataset and may have PIDs assigned to component parts or individual records within it. Digital Object Identifiers (DOIs) are common PIDs used in this way. A PID is an unchanging, searchable identifier which allows for the easy retrieval of data, as well as tracking of publications that use or cite a dataset. Note that dedicated PIDs exist for physical samples (International Geo-Sample Number or IGSN) and other classes of data, not only digital data, and should be used where available.

(20) Data requiring Mediated Access must also include terms of use specifying how the Data may be reused (e.g., prohibition against redistributing sensitive datasets). Data should remain as reusable as possible. Other datasets may also have terms of use specified (with appropriate justification). The Macquarie University Data Access Agreement is provided as a default terms of use. Consult a Research Data Steward for further information.

(21) If no Data Outputs are being disseminated, dataset-level Metadata should be lodged with the Macquarie Research Data Repository, unless exposure of the Metadata itself reveals Sensitive Information. Any request to keep Metadata private must be justified.

(22) Disseminated data may be subject to an embargo period, typically of eighteen (18) months, to allow Researchers time to publish results before making Data public.

Data Protection

(23) Researchers must consult the Research Data Sensitivity, Security and Storage Guideline to determine the minimum-security measures to be applied during data management together with any terms of applicable research agreements (including but not limited to a Data Access Agreement). Additional security provisions may be required for defence related research projects (following Australia's Foreign Relations (State and Territory Arrangements) Act 2020).

(24) A Data Breach occurs when personal information or Sensitive Information collected during research is lost or subjected to unauthorised access or disclosure. A Researcher has a responsibility to initiate appropriate remedial action reducing the likelihood of serious harm occurring from the inappropriate use of, access to, or loss of Data containing personal or Sensitive Information. In addition to privacy breaches related to personal data (refer Privacy Policy), Data Breaches may also involve sensitive commercial-in-confidence data, sensitive trade, military or environmental data that may have serious consequences if released. The Researcher must report the data security breach immediately according to the Data Breach Policy and to other relevant parties including the relevant Human Research Ethics Committee. Note that reliably reporting a Data Breach in a timely fashion requires the use of infrastructure with appropriate security, auditing, and alerts – a principal reason why Researchers must use supported University platforms or develop alternative mitigation approaches.

(25) If external service providers are used for collection, management, collaboration, analysis, archiving, or dissemination of sensitive or highly sensitive data, the platform must be approved by a Research Data Steward or by the Human Research Ethics Committee as part of a Data Management Plan being submitted. It is the responsibility of the Researchers to provide the information necessary to assess the platform's suitability. Platforms must allow Researchers and Macquarie University to comply with relevant legal, ethical, funder and publisher requirements, and provide data security and privacy comparable to research data systems approved by the University.

Data offboarding

(26) When leaving Macquarie University, Graduate Research students, research staff, and Researchers must make arrangements for the ongoing custody of Research Data for which they were responsible in accordance with the Retention and Disposal Procedure). This involves, but is not limited to: thoroughly documenting all datasets; designating data custodian and owner; reviewing all contractual, approval, and data sharing agreements, ensuring adherence to regulatory requirements including those related to Data Retention, disposal; retaining/archiving data on the institution infrastructure in accordance with the Records and Information Management Policy; and updating applicable Data Management Plans (DMP).

Section 4 - Guidelines

(27) Refer to the Research Data Sensitivity, Security and Storage Guideline.

Section 5 - Definitions

(28) The following definitions apply for the purpose of this Policy:

a. Breach means a failure to meet the principles and responsibilities of the Macquarie Research Code (including failing to meet the standards or Policies accompanying the Macquarie Research Code). Breaches occur on a spectrum from minor to more serious Breaches. A serious Breach of the Macquarie Research Code which is also intentional or reckless or negligent constitutes research misconduct.

b. CARE Principles address and ensure that Indigenous rights are enacted in the use of Indigenous Data and uphold the knowledge authority of the Indigenous peoples and the purpose behind the data. The term 'CARE' stands for Collective benefit, Authority to control, Responsibility, and Ethics.

c. Data or Research Data may differ from discipline to discipline. Data means any information, sources, facts, observations, experiences, measurements, or materials that are generated, collected, collated or used in the conduct of research for purposes of substantiating research scholarship and findings. This may include, but is not limited to, information or primary and secondary materials held in any digital format or media, or anything that can be digitised, on which an argument, theory, test or hypothesis, or another Research Output is based. Data may also include other 'digital research objects' such as analytical code that support research outcomes. Research data may be in the form of facts, observations, images, computer program results, recordings, questionnaires/surveys, biographies, audio files, physical specimens or artefacts, measurements, experiences or various other forms. Data may be numerical, descriptive, visual or tactile and could be raw, cleaned or analysed.

d. Data referred to in this Policy does not include the information about research performance or statistical research data which is used by Macquarie University for planning and budget purposes or that which is reported to government agencies, e.g., Excellence in Research for Australia (ERA).

e. Data Access Condition may include specific restrictions on how people can gain access to the Data Output and should be determined by the sensitivity of the information.

f. Data Breach is the accidental or deliberate access or exposure of Macquarie University information (including Research Data) to unauthorised parties. Potential or actual Data Breaches must be reported appropriately in accordance with the Data Breach Policy and the Cyber Security Policy.

g. Data Dissemination refers to making data available to a wider audience through traditional (e.g., publishing in a trusted Data Repository) or non-traditional (e.g., database, collection, registry, exhibition, social media, website) methods. Ultimately, data is shared so it can be reused.

h. Data Lifecycle refers to the various stages that data goes through from initial creation or capture to eventual archiving, publishing and/or re-using. Data have a longer lifespan than the project that creates them, and there is a need for all stages of the data lifecycle to be planned.

i. Data Management Plan describes the management of data through all stages of its lifecycle and includes documentation of how data will be created, collected, stored, and managed, and the provisions for access to data from its creation or collection to its preservation (refer to the Research Data Management Procedure).

j. Data Output refers to any output that communicates, disseminates, or makes available the Research Data to the public or to other researchers. Data outputs may include digital data assets, techniques, algorithms, and software. Data outputs should be deposited in a Data Repository with appropriate Data Access Agreement and terms of use.

k. Data Repository is information infrastructure, which may also be known as a data library or data archive. A Data Repository is used to store data for the long term and often supports data sharing or publication (open or Mediated Access) and data reuse reporting. Data outputs should be deposited in a domain-specific, domain-general, or institutional data repository. The submission of a Data Output into a data repository is often a requirement for publication or funding. Data repositories differ in their ability to offer users the ability to set Mediated Access conditions. Research data containing sensitive information that is being deposited into an online repository should have appropriate Mediated Access conditions assigned to it (refer to 'Mediated Access' or 'Specialised Access' in the Research Data Sensitivity, Security and Storage Guideline. A restrictive license is also applied that limits redistribution of the data.

l. Data Retention refers to the length of time that data and records are kept after research project completion for the purpose of meeting legislations, funders, organisation, and other requirements.

m. Data Security refers to the process of protecting data from unauthorised access and data corruption throughout all stages of its lifecycle. This may include practices such as: data encryption, two factor authentication, backup and other key management practices that protect data across all applications and platforms. Refer to the Research Data Sensitivity, Security and Storage Guideline.

n. De-identified or Anonymised Data: These terms are often used interchangeably, but for the purposes of this Procedure:
    i. De-identified Data refers to data which has had any direct and indirect identifying details (eg personal or locational) removed or transformed to protect privacy or confidentiality. However, identifying information may be able to be re-associated with the data later or re-identification may be possible in association with other publicly available data.
    ii. Anonymised Data refers to data which has been collected or processed in a manner that makes it permanently impossible to identify individuals or locations from it. This usually involves stripping all identifiable elements from the data, for example, by aggregating or summarising the data to such a general level that individuals or locations cannot be identified, and the data cannot be re-engineered to identify individuals or locations.

o. FAIR Data Principles are implemented to enhance and improve the findability, accessibility, interoperability, and reusability of data and relate to the machine-actionability of the data (i.e., the capacity of computational systems to find, access, interoperate, and reuse data with none or minimal human intervention). They should be considered and reflected in the management of data.

p. Indigenous Data encompasses information or knowledge, including data on Indigenous lands, resources and environment, data about Indigenous peoples, data about Indigenous languages, cultural practices and cultural heritage and data from Indigenous peoples or communities, in any form, that pertains to and may impact Indigenous peoples both collectively and individually.

q. Intellectual Property (IP) includes all copyright and all rights in relation to inventions (including patent rights), registered and unregistered trademarks (including service marks), registered and unregistered designs, confidential information, and circuit layouts and all other intellectual property rights resulting from intellectual activity in the academic, industrial, scientific, literary, and artistic fields recognised in domestic law anywhere in the world.

r. License offers researchers and institutions a standardised way of sharing Data Outputs with others and understanding their rights to use a Data Output generated by other researchers without infringing copyright. When a Data Output is being produced at Macquarie University, a licence (such as one that is defined by the Creative Commons) should be assigned, which sets out the uses that may lawfully be made of the Data Output, and specifies the conditions under which its future use must comply.

s. Macquarie Research Code (Macquarie University Code for the Responsible Conduct of Research) sets out the principles that underpin an honest, ethical, and conscientious research culture and the expectations for the conduct of research under the auspices of Macquarie University.

t. Macquarie Research Data Management Policy (Research Data Management Policy) outlines the expected approach to the collection, storage, sharing, and dissemination of research data or information that facilitates reuse of data by the research community, while honouring ethics or confidentiality requirements and any contractual obligations imposed on Macquarie University by its sponsors, collaborators, partners, third-party providers, or funding bodies.

u. Mediated Access data has been deposited in a repository but requires a request from any would-be user, followed by the granting of permission for the use of the data either from a representative of the repository (e.g., ‘restricted access' data in the Macquarie Research Data Repository) or from the researcher(s) who produced the data, typically the designated Data Custodian (e.g., 'special access' data in the Macquarie Research Data Repository).

v. Metadata refers to documentation that is created throughout the data lifecycle. Metadata is essential information describing data, providing the context for a Data Output, and making the data discoverable and reusable.

w. Primary Materials refer to data, information, or physical materials (see Data definition) generated, created or collected by researchers in the course of research conducted during study, project, employment, or appointment with Macquarie University.

x. Researcher is any person (or persons) who conducts or assists with the conduct of research under the auspices of Macquarie University - may include staff members (academic and professional), visiting students, visiting fellows, volunteers, honorary and adjunct title holders, Emerita/us Professors, occupational trainees, and any student in any course at the University who conducts or assists with the conduct of research at or on behalf of the University.

y. Research Data - see Data.

z. Research Output refers to any output that communicates, disseminates, or makes available the products of research. A Research Output may include any form (hardcopy, electronic, creative work or other) of academic or public communication of the research from any stage of the research process (e.g., a professional blog, web-based publications, books, performances, book chapters, conference papers, journal articles or Data Outputs).

aa. Sensitive or Highly Sensitive Information refers to information of a personal or sensitive nature that must be protected against unwarranted disclosure. Refer to the Research Data Sensitivity, Security and Storage Guideline for guidance in assessing the sensitivity of data and appropriate security measures to be applied. Sensitive information may include, but is not limited to, health-related data; personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; financial information; genetic data or biometric data processed solely to identify a human being. Sensitive information may also relate to heritage or cultural information or information that may pose a risk to the environment or animals (such as the location of endangered species). Sensitive information must be safeguarded with appropriate Data Security practices following the Research Data Sensitivity, Security and Storage Guideline. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy (refer to the Privacy Policy), for the protection of animals or the environment or for proprietary considerations.

Status and Details

Status	Current
Effective Date	5th February 2026
Review Date	5th February 2031
Approval Authority	Deputy Vice-Chancellor (Research)
Approval Date	4th February 2026
Expiry Date	Not Applicable
Responsible Executive	Sakkie Pretorius Deputy Vice-Chancellor (Research) +61 2 9850 8645
Responsible Officer	Kandy White Director, Research Ethics and Integrity +61 2 9850 7854
Enquiries Contact	Mahdieh Dashtbani Moghari Manager, Research Data Management