Research Data Management Procedure

Section 1 - Purpose

(1) This Procedure documents the expected practices for research data management, including data collection, storage, use, sharing, and retention 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, 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 from which it will be obtained, should be reported, along with relevant contractual details;
b. when data is produced by a collaborative research project with researchers outside of Macquarie University, a Data Access Agreement or Collaborative Research Agreement (or equivalent) should be entered into by all parties. This agreement should detail ownership and arrangements for custodianship, storage, retention, access, licensing, use / reuse of the data, and the right to produce research outputs based upon the data. This agreement can take a variety of forms. Projects may use a standard Macquarie University Agreement, or another agreement approved by the researchers and a Research Data Steward at Macquarie University (or approved as a standard annexure to a research contract administered through Research Services); and
c. researchers wanting to share their active data with external parties should ensure all parties enter a Data Access Agreement or a Collaborative Research Agreement which specifies access, use and governance conditions (refer to the Macquarie University Collaborative Research Standards).

Data Management Planning

(7) All researchers must clearly establish their intentions related to each stage of the data life cycle 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 life cycle, 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 apply, to the extent possible, the Findable, Accessible, Interoperable, and Reusable (FAIR) 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 Higher Degree Research (HDR) candidate 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);
    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);
    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;
    v. being undertaken by a HDR candidate 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 various cohorts between 2021 to 2024.
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) Permanent retention of data through deposit of data outputs into a discipline-specific repository or the Macquarie University Research Data Repository is best practice for all projects. Retention is required where the data is 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 data set of acceptable quality and useability, 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) The significance of research data is not always immediately apparent and permanent retention should be considered the default. If data is not retained permanently, the reason for its disposal should be explained in the DMP, and its disposal protocol should be articulated. The retention period must not be less than the period specified by prevailing standards for the specific type of research and any applicable state, territory or national legislation. For example, 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 twenty (20) 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.

(11) 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 2023 and any legal requirements and as appropriate for the design of the research.

(12) 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

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

(14) 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.

(15) Data Outputs should conform to the FAIR data principles as far as possible and any relevant discipline-specific metadata guidelines or practices. Appropriate context (descriptive, technical, methodological, and access information) should be provided, either within the data or in a separate metadata record for the data.

(16) Data should be disseminated, regardless of whether the data directly supports the research findings. Such data should be as comprehensive as possible. Data should be as open as possible, and only as closed as necessary to meet ethical, contractual or intellectual property requirements (cf. EU Horizon 2020). Any request not to disseminate data must be justified.

(17) 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. Doing so could involve removing sensitive information from the data, aggregating data, de-identifying data, or 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.

(18) Data that is being disseminated (a ‘data output’):

a. must be deposited in a discipline-specific, general-purpose, or Macquarie University research data repository, or in national or international 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 output. 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. 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 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; 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;

(19) 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 Standard License Terms and Conditions of Use is provided as a default terms of use. Consult a Research Data Steward for further information.

(20) 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.

(21) 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

(22) 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 defense related research projects (following Australia's Foreign Relations (State and Territory Arrangements) Act 2020).

(23) 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, 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 to Macquarie University IT Service Desk 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 endorsed University platforms or develop alternative mitigation approaches (see clause 24). The Chief Risk Officer and IT will coordinate with the Privacy Officer (as required).

(24) 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.

Section 4 - Guidelines

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

Section 5 - Definitions

(26) Definitions specific to this Procedure are contained in the Research Data Management Policy.

Status and Details

Status	Current
Effective Date	6th September 2021
Review Date	7th September 2024
Approval Authority	Deputy Vice-Chancellor (Research)
Approval Date	3rd September 2021
Expiry Date	Not Applicable
Responsible Executive	Sakkie Pretorius Deputy Vice-Chancellor (Research) +61 2 9850 8645
Responsible Officer	Shawn Ross Director, Digitally Enabled Research +61 2 9850 7010
Enquiries Contact	Shawn Ross Director, Digitally Enabled Research +61 2 9850 7010