

RESEARCH DATA MANAGEMENT POLICY

Section	Research Management
Contact	Office of the Provost
Last Review	November 2024
Next Review	November 2027
Approval	SLT 24/11/129
Effective from	November 2024

Background

Massey University recognises significant value in the data generated by its researchers, creative practitioners, and research students. Durable research data is essential to justify and defend the outcomes of research and can also have ongoing value for other researchers and the wider community. Increasingly data sharing is encouraged or required by research funders, data providers and publishers. Well-organised, well-documented, preserved, and shared data are valuable resources to advance academic inquiry and the impact of research, and to increase opportunities for learning and innovation.

Research data management is the process of planning and undertaking the collection, organisation, storage, backup, preservation and sharing of data and primary materials, throughout the research lifecycle, for current and future research purposes and uses. Good data management practices increase transparency, reduce the risks of data loss, facilitate appropriate re-use and sharing of data, enhance transparency and accountability, minimise privacy breaches, reduce reputational harm to researchers/institutions, enhance integrity of research, and support investment decisions on digital and physical infrastructure.

Purpose

The purpose of this policy is to articulate the responsibilities of the University community for the management of research data. The policy:

- Describes principles for ensuring the safe, secure and traceable storage and management of research data.
- Explains the University's expectations in relation to the management of research data including the responsibilities of researchers, research students, Heads of Units, and the University
- Facilitates University-wide planning for the development of digital and physical storage infrastructure, systems and support services to enable the efficient and effective management of the University's research data assets.
- Supports the University's commitment to being a Te Tiriti-led organisation and provides for the appropriate governance of Māori data.
- Provides for the appropriate governance of Pacific data.
- Positions the University for current and emerging data management issues including the sharing and re-use of publicly funded data collections, and legal, ethical and protective security requirements for research data, and
- Advances the principles of research integrity by ensuring research outcomes are founded on relevant information capable of verification and review.

This policy applies to staff, students, supervisors, and other members of the Massey University who are involved in

the collection, creation, re-use and/or management of research data.

Policy

1. Research data

1.1 Research data is any information that has been collected, observed, generated, analysed or created to validate original research findings. Data may be numerical, textual, audio-visual, digital or physical, depending on the discipline and the nature of the research. It may be raw, cleaned or processed, and may be held in any format or media.

1.2 Research data may include:

- laboratory and field notebooks
- primary research data (including machine data in hardcopy or computer readable form)
- databases
- clinical data, including clinical records.
- completed questionnaires, and interview and observation data.
- photographs
- audio-visual material
- journals or visual diaries
- test responses
- drawings, or
- physical collections of slides, artefacts, manuscripts, specimens or samples.

2. Research Data Management Plans

2.1 Making decisions early in the research process about how data will be managed has benefits for researchers and research students, and for the University as a whole. Research Data Management Plans provide for the efficient and responsible storage, governance and disposal of research data.

2.2 A Research Data Management Plan is required for research projects involving the collection, creation or reuse of sensitive or restricted research data, or where this is required by the University, a funder, an ethics approval process, or other external party.

2.3 Research Data Management Plans must comply and be consistent with any relevant national or international research funding requirements/contract and with ethics approval for the research project.

3. Ownership and custodianship of research data

3.1 Data ownership refers to the intellectual property rights over the data collected, created, or re-used through research, and may also define rules around data management and use. Ownership may be influenced by funding agreements, commercial potential, and contractual obligations.

3.2 Where the research is carried out at multiple organisations or with external collaborators, and where there are no formal agreements or requirements, ownership of research data should be clarified as soon as possible and recorded in writing.

3.3 Ownership of intellectual property is governed by Massey's Intellectual Property Policy.

3.4 Researchers and research students working with Māori data should be aware of and support Māori data sovereignty, and the relevance of managing and sharing data in accordance with the CARE Principles for Indigenous Data Governance¹.

3.5 Researchers and research students working with Indigenous data including Pacific data should be aware of the relevance of managing and sharing data in accordance with the CARE Principles for Indigenous Data

¹ <https://www.gida-global.org/care>

Governance.

4 Data sharing and transfer

- 4.1 Researchers and research students are encouraged to share research data and primary materials during their research, at publication and at completion, subject to any ethical, contractual, intellectual property, cultural, privacy or confidentiality requirements.
- 4.2 To transfer digital research data or records, researchers and research students should use University licensed file transfer and cloud services or other secure services as advised by Massey's Information Technology Services.

5 Storage, retention, and disposal of research data

- 5.1 Sufficient metadata must be recorded to ensure research data are discoverable, and in such a way that metadata can be understood independently without recourse to the creator. Metadata for digital and digitisable data should be designed to meet the FAIR principles to make research data more discoverable.
- 5.2 Unless otherwise specifically agreed, research data will be retained by the researcher or research supervisor: (a) in their academic unit or College or as otherwise required by the University, or (b) in the case of digital data, on University-managed storage infrastructure.
- 5.3 Research data will be retained in an accessible form in accordance with the requirements of this Policy, for the retention period specified in a funder agreement or contractual arrangement or research ethics approval or in a Research Data Management Plan or as otherwise required by the University.
- 5.4 At the end of the retention period, researchers and research supervisors may make a recommendation to their Head of Academic Unit to archive or destroy the research data.
- 5.5 Where it can be shown that there are no specific arrangements (including funder agreement or contract, research ethics approval, Research Data Management Plan or other University retention provision) associated with a collection of research data, the research data and its supporting metadata may be destroyed with the approval of the appropriate Head of Academic Unit or as otherwise specified by the University.
- 5.6 Physical or non-digital forms of research data created after the commencement date of this policy should be digitised promptly where possible. Where there is no requirement to retain the original physical research data, a recommendation for its destruction may be made in accordance with Section 5.4.
- 5.7 Data (including physical data) with archival, historical or other long-term value shall be properly curated to remain accessible and usable for future research and should not be disposed of or destroyed without justification and approval of the appropriate Head of Academic Unit or as otherwise specified by the University.
- 5.8 Arrangements for the ongoing storage on University property of physical data that cannot or is not digitised, and that has not been identified as having long-term value under Section 5.7, must be agreed between Heads of Units and researchers, or research supervisors in the case of research students, or as otherwise required by the University. Such arrangements must have an identified retention period after which time the agreement will be reviewed, or a recommendation for its destruction may be made in accordance with Section 5.4.

6 Responsibilities

6.1 General responsibilities

- 6.1.1 Research data management is a shared responsibility. Researchers, academic units and administrative and service units should work in partnership to implement good practice.
- 6.1.2 The University is responsible for ensuring the safe, secure and traceable storage and management of research

data.

6.1.3 All staff and students engaged in research have a responsibility to manage research data well, by addressing ownership, storage and retention, and access, over and beyond the end of the research project.

6.1.4 Researchers and research students (in consultation with their research supervisors) are responsible for ensuring that sufficient data and primary materials are retained to justify the outcomes of research and, if necessary, defend them against challenge.

6.2 Specific responsibilities

University responsibilities	<ul style="list-style-type: none"> • Communicating the requirements of this policy and facilitating its adoption through the provision of guidance and support. • Providing the necessary infrastructure, supporting resources and advisory services to enable researchers, research students and research supervisors to meet their responsibilities for research data throughout the research data lifecycle. • Providing advice and guidance on issues connected with good data management, such as data protection, research integrity, research ethics and intellectual property rights.
Researcher responsibilities	<ul style="list-style-type: none"> • Creating and updating required Research Data Management Plans. • Recording and retaining the data underpinning their research in a durable and appropriately referenced form. • Where the research is carried out at multiple organisations or with external collaborators, ensuring that there is written agreement between all relevant parties that specifies clearly the arrangements for storage, retention and destruction of research data within each organisation. • Arranging for the prompt digitisation of physical (non-digital) data where possible. • Ensuring arrangements for sharing, archiving, long-term storage/curation or destruction of data once the project has been completed. • Making appropriate arrangements if they require and have rights to continued access to research data after leaving the University.
Research supervisor responsibilities	<ul style="list-style-type: none"> • Providing guidance and support to research students on the application of this policy to research projects. • Supporting their research students in creating and updating Research Data Management Plans. • In consultation with their research students, establishing and documenting the ownership of research data and agreed exit procedures.
Research student responsibilities.	<ul style="list-style-type: none"> • With the support of their researcher supervisors, creating and updating required Research Data Management Plans. • Recording and retaining the data underpinning their research in a durable and appropriately referenced form. • In consultation with their research students, establishing and documenting the ownership of research data and agreed exit procedures.
Heads of Academic Units	<ul style="list-style-type: none"> • Overseeing the appropriate archiving or destruction of research data at the end of the retention period. • In consultation with the researcher, agreeing appropriate storage or destruction of physical data on University property that cannot or should not be digitised or archived once the project has been completed.

Definitions

The following definitions apply to this document:

CARE principles refer to the principles for indigenous data governance (Collective benefit, Authority to control, Responsibility and Ethics) published by the Global Indigenous Data Alliance.

Data governance refers to the arrangements put in place to ensure the interests of rightsholders and stakeholders in research data are protected and that all ethical, legal, data sovereignty and commercial constraints are adhered to throughout the research data lifecycle.

Destruction means the process of overwriting, erasing or physically destroying information so that it cannot be recovered.

FAIR principles are a set of community-developed guidelines to ensure that data or any digital artefacts are Findable, Accessible, Interoperable and Reusable. The principles can be applied to digital data and artefacts from any discipline.

Māori data refers to the digital or digitisable information or knowledge that is about or from Māori people, language, culture, resources, or environments.

Māori data sovereignty refers to the inherent rights and interests of Māori in relation to the collection, ownership, and application of Māori data.

Metadata means structured or schematised information about the attributes of an item or collection that enables that item or collection to be identified, retrieved and managed over time. Metadata may include descriptions, details of provenance, structure and location, and other information which could aid comprehension and re-use.

Pacific data refers to digital or digitisable information or knowledge that is about or from Pacific people, language, culture, resources, or environments.

Research data has the meaning given in Section 1 of this policy.

Research data lifecycle means the various stages of creating the data, from point of creation or collection through to dissemination. The research data lifecycle typically continues beyond the research project during which the data was created.

Research Data Management Plan means a document that provides information for the efficient and responsible storage, governance, and disposal of research data.

Research student means any person enrolled in a degree, diploma, or certificate course at the University whose enrolment includes undertaking research of at least 90 credits.

Research supervisor has the meaning set out in Massey's Policy for Doctoral Supervision and [Master's supervision].

Researcher includes research staff, honorary appointees, adjunct appointees, and contractors that undertake research at the University or using University resources, or otherwise on behalf of the University.

Restricted research data has the meaning in the New Zealand Government's classifications for information security.

Retention means to retain research data in accordance with the General Disposal Authority for New Zealand Universities.

Sensitive research data has the meaning in the New Zealand Government's classifications for information security.

Trusted Research-Protective Security Requirements Guidance refers to the guidance developed by Te Pokai Tara Universities New Zealand the eight New Zealand universities to manage risks relating to research activities including the misappropriation or misuse of intellectual property, sensitive research, and personal information.

Relevant legislation:

Copyright Act 1994
Health Information privacy Code 2020
Official Information Act 1982
Privacy Act 2020
Public Records Act 2005

Related policies and procedures:

Code of Responsible Research Conduct
Code of Ethical Conduct for Research, Teaching, and Evaluations Involving Human Participants
Code of Ethical Conduct for the Use of Animals for Research, Testing, and Teaching
Data Management Policy
Device Security Policy
General Disposal Authority for New Zealand Universities
Information and Technology Security Policy
Information and Records Management Policy
Intellectual Property Policy
Official Information Policy
Policy for Doctoral Supervision
Thesis Embargo Policy
Privacy Policy
Research and Consultancy Activities Policy
Research and Consultancy Activities Procedures
Health Information Privacy Code 2020

Document Management Control:

Prepared by: Research Management
Authorised by: Office of the Provost
Approved by: SLT 24/11/129
Date issued: November 2024
Last review: November 2024
Next review: November 2027