Research Data Management Procedure

Version 3 - Reconfirmed 1 November 2024

Contents

Purpose

This procedure describes how research data is managed by the University, consistent with the *Australian Code for the Responsible Conduct of Research 2018* (the Code), other relevant legal instruments and research guidance frameworks including the requirements for:

a) data management planning

b) record keeping

c) classification of data

d) storage

e) retention and long-term data preservation

f) sharing and reuse of research data.

Applicable governance instruments

Instrument	Section	Principles
Research Policy	2 Responsible conduct of research	2.1-2.2
	4 Research data and output	4.1-4.2

Intellectual Property Policy	2 Ownership and assignment	2.1-2.2
	4 Indigenous Cultural and Intellectual Property Rights	4.2
	5 Copyright	5.1
Data and Information Governance Policy	1 Privacy	1.2-1.5
	2 Cyber security	2.1
	4 Data and information management	4.1-4.4
Australian Code for the Responsible Conduct of Research 2018	All	N/A
Management of Data and Information in Research: A guide supporting the Australian Code for the Responsible Conduct of Research	All	N/A
AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research	All	N/A
Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: guidelines for researchers and stakeholders	All	N/A
National Statement on Ethical Conduct in Human Research (2007, updated 2018)	All	N/A
Privacy Act 1988 (Cth) *Personal Information Protection Act 2004* (Tas) *Copyright Act 1968* (Cth)	All	N/A

Procedure

1. Background

1.1. This procedure applies to the management of research data (including primary materials). Research data is the facts, observations, measurements, and experiences on which an argument, theory or test is based.

1.2. Research data can be numerical, descriptive, or visual and raw or analysed, experimental or observational. It includes laboratory notebooks, field notebooks, primary research data, questionnaires, audiotapes, videotapes, models, photographs, films, test responses, and any other records that are necessary for the reconstruction and evaluation of the reported results of research.

1.3. Under the Code, University researchers are responsible for managing their data. The objectives of this procedure are to ensure that research data is managed in a way that:

a) complies with all relevant laws, regulations, and guidelines.

b) complies with privacy, ethical, contractual and publication requirements.

c) is consistent with copyright or licensing arrangements in place including any external research partner or funding agency (e.g., National Health and Medical Research Council (NHMRC) and Australian Research Council (ARC)).

d) aligns with discipline-specific practices and standards for research.

1.4. This procedure supports the University's commitment to FAIR and CARE data principles The FAIR principles ensure research data is Findable, Accessible, Interoperable, and Reusable, promoting efficient data management and sharing. The CARE principles emphasise ethical considerations and Indigenous data sovereignty, guiding the responsible use and management of Indigenous peoples' data.

1.5. This procedure does not apply to business and operational records related to research covered by the *Information Management Procedure* or research outputs which are covered by the *Publication and Dissemination of Research Procedure* and the *Open Access Procedure*. Data generated and produced during learning and teaching activities that is later used in research is considered research data.

1.6. Contacts for further guidance and support are listed in Schedule B.

2. Ownership of research data

2.1. Data Owners have the ultimate authority to determine how data is managed including storage, retention, disposal, publication or licensing arrangements and the recipients of any proceeds if the research data is commercialised.

University owned data

2.2. In accordance with the University's *Intellectual Property Policy* the University owns all research data created by an employee (excluding copyright material in scholarly works) in the course of their employment duties, subject to exceptions including:

a) Data from or about Aboriginal and Torres Strait Islander peoples is owned by those peoples per the data sovereignty principles of the *AITSIS Code of Ethics for Aboriginal and Torres Strait Islander Research* (see also section 2.3)

b) Intellectual property created by students, including Higher Degree by Research students, is owned by the student, subject to any agreement by the student to assign ownership.

c) Data for which ownership has been explicitly assigned or transferred to another individual, group, or organisation by contract.

Research involving Indigenous people, their culture or heritage

2.3. Where research involves indigenous people, their culture or heritage, decisions regarding management of research data are subject to the following:

a) *The AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research and Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: guidelines for researchers and stakeholders* or equivalent guidelines in local jurisdictions.

b) Indigenous Cultural and Intellectual Property (ICIP) Rights (in addition to other copyright and intellectual property requirements).

c) The CARE principles to ensure appropriate and respectful regard for Indigenous data sovereignty.

d) Consultation with Indigenous owners prior to making decisions regarding access to or reuse of data or information.

e) Consideration of the appropriate ways of collecting, storing, and accessing the data, and communication with research participants and data managers regarding these issues.

Research data owned by third parties

2.4. Where University researchers are accessing or using third party data, ownership, access, management, and reuse of the data will be documented in a formal data sharing agreement (or equivalent) or an informal data management plan.

3. Data management and planning

3.1. All data and primary materials must have an identified 'data steward' responsible for the day-to-day management of the research project. The data steward for a research project is ordinarily the chief investigator. Where a data steward cannot be identified, the role will be filled by the relevant Head of Organisational Unit or their nominee.

Data Management Plans

3.2. As early as possible in a research project, the data steward should develop a data management plan (DMP). The contents of a DMP depends on the type of research, but generally describes the following:

a) the types of data that will be generated by the project

b) classification of the data (see section 5)

c) storage and access requirements

d) use and analysis of the data

e) retention, and disposal, sharing, re-use

f) licencing of data and information

g) potential risks (such as data loss or corruption) and mitigation strategies (including security requirements)

h) data ownership and exit planning

i) contractual obligations or other restrictions that may apply during the life cycle of the project.

3.3. Where data will result from research involving human participants, the DMP must also comply with clauses 3.1.44-50 of the National Statement on Ethical Conduct in Human Research, including recording the details of consent obtained from participants and any conditions on their consent.

3.4. Where the data involves Indigenous people, their culture or heritage, the DMP must also consider the requirements of section 2.3 of this procedure.

3.5. For multicentre or collaborative research projects, the data steward will ensure agreements are in place for managing data in accordance with the *Collaborative Research Procedure*.

3.6. The data steward must update the DMP as required over the course of the research project, and ensure that data management planning documentation is kept with other research project documentation or stored with the research data.

Costs of Data Management

3.7. Costs associated with data management and retention (including data storage beyond the life of the project) must be included in the project budget, and approved in accordance with the relevant Organisational Unit requirements, or if externally funded, in accordance with the *Research Funding Costing Procedure*.

3.8. In planning and costing the data storage and management infrastructure required for a project, researchers should consult with Digital Research early in the research planning stage to ensure their planned research data management is feasible.

4. Record keeping and metadata

4.1. Researchers are responsible for clear and accurate recordkeeping throughout the life cycle of their research. Researchers are required to:

a) Maintain accurate and complete records of their research data, including metadata (see below) methodologies, and analytical processes, to ensure the research can be understood, verified, and reproduced.

b) Retain and produce on request all relevant approvals, authorisations, and other administrative documents, such as ethics approvals, agreements (such as data transfer agreements and licences) and consent forms.

c) Keep accurate records, such as through the DMP, of where research data, primary materials, metadata and information pertaining to their research is stored.

d) Where data is owned by a third party or has been obtained by the University from a limited access database, keep records as to the location of the original data and any ongoing ownership, access, and re-use requirements.

Metadata

4.2. Metadata is the information that describes, documents, and contextualises research data, including details about data collection, methodology, provenance, and usage rights. Metadata is essential for data discovery, interpretation, reuse, and long-term preservation. It ensures that data remains understandable and accessible to both current and future researchers, in line with FAIR data principles.

4.3. Researchers will store metadata alongside the research data, ensuring that it is easily accessible, associated with the relevant dataset, and to support future data management and reuse.

4.4. There are three main classes of metadata that should be described for any given dataset:

a) Descriptive metadata: information that helps users discover and identify data, such as title, author, keywords, and abstract.

b) Structural metadata: information about the organisation and relationships between data elements, such as hierarchical structure, data formats, and data models.

c) Administrative metadata: information related to the management and administration of data, such as rights management, access restrictions, data provenance, and preservation history.

4.5. Researchers should use established metadata standards relevant to their discipline to ensure interoperability and data reusability. Guidance on relevant metadata standards and repositories is provided by the Library.

5. Data classification

5.1. The University's Data Classification Framework (see Schedule A) can be used to categorise data into one of the following four categories based on the likelihood of harm if there is a data breach or the data is misused:

a) Green - data misuse would have little or no impact.

b) Yellow – data misuse unlikely to cause harm, most likely will have a negligible impact.

c) Orange – data breach or misuse may adversely impact the University or an external party and could be a regulatory offence.

d) Red – data breach or misuse expected to cause serious harm to the University or an external party and could constitute a regulatory or criminal offence.

5.2. Researchers will ensure that measures taken to protect the security and privacy of data are proportionate to the risks. Based on the classification, IT services can make recommendations as to how the data should to be stored, the measures required to protect the security and privacy of the data, access requirements and whether and how the data can be shared.

5.3. Researchers are responsible for ensuring that research data is classified into one of the four categories initially as part of the data management planning process and then as data is generated throughout the research.

5.4. Where research data is classified as Red, researchers must advise Digital Research prior to initiation of the research and obtain approval for the planned data handling processes.

5.5. Researchers should re-classify data where the data is transformed during the course of their research, for example if the data is deidentified following analysis or a data set transformed.

6. Storage of research data and primary materials

6.1. The University will provide access to facilities for the safe and secure storage of research data and primary materials. Where possible and appropriate, research data and primary materials will be stored using University provided or manage options, taking into consideration the Classification of the information being stored, contractual obligations, and any access requirements. Digital Research can provide additional guidance and advice.

6.2. Researchers are responsible for ensuring:

a) research data and primary materials are kept in a safe and secure environment and that research data is stored in a retrievable way.

b) costs associated with accessing data storage and management facilities are budgeted for in accordance with section 3.7 of this procedure.

c) access permissions and other relevant data protections are in place and appropriate for the classification of the data and any ethics requirements, contractual obligations etc have been met.

Digital Research can provide additional guidance and advice.

6.3. Where research data needs to be stored or hosted using external providers, these systems are required to comply with University policies and procedures. A cyber security and risk assessment may be required as per the *Cyber Security Controls Procedure*.

6.4. Orange or Red data should not be transferred to non-approved cloud or externally hosted platforms without approval from the Chief Information Officer as per the *Cyber Security Controls Procedure*.

6.5. To optimise project efficiency and avoid information loss and duplication, researchers should employ good data management practices across all data storage locations. Practices will vary between disciplines, but always include appropriate password protection, stable storage formats, integrity checking mechanisms and regular backup of critical data as well as comprehensive metadata that is updated and stored with the primary data (see section 4).

6.6. After the active phase of research is completed, or where there is no need to retain the research data and primary materials within the organisational unit, researchers will work with their organisational unit to arrange for secure long-term storage of their research data and develop a plan for ongoing preservation and curatorship of that data. Dataset archiving to encrypted tape storage is provided by Digital Research. When selecting the storage option, researchers are encouraged to follow FAIR data practices, such as facilitating data reuse by publishing their data in a discipline-specific repository or using the University's Research Data Portal.

7. Retention and long-term data preservation

7.1. The general principle is that data and primary materials will be appraised, archived, and retained for the longest possible retention period, unless there is a reason (such as the conditions of ethics approval, contractual obligations, or legislative requirements) mandating that some data or materials must be destroyed.

7.2. Researchers are responsible for determining the minimum retention periods that relate to their research data. Guidance is provided in the University's Records Retention and Disposal Schedule (DA 2398) or by contacting the Information Management Unit.

7.3. In general, the minimum retention period is five years post-publication, but depends on consideration of the following:

a) the requirements of the local jurisdiction for research outside of Tasmania

b) the discipline and type of research (e.g. clinical trials)

c) University requirements (such as requirements related to person information and privacy)

d) indigenous data governance principles

e) requirements of bodies such as funding agencies, commercial sponsors, government bodies and publisher

f) legislative requirements (including the *Australian Code of Responsible Conduct in Research (2018)* and the *Archives Act 1983* (Tas))

g) any contractual requirements.

7.4. Considerations for maintaining data and primary materials beyond the minimum retention period include:

a) uniqueness and non-replicability

b) reliability, integrity, and usability

c) relevance to a known research initiative or collection

d) community, cultural or historical value

e) economic benefit

f) value of the data or material for further research.

7.5. Decisions relating to the retention of primary materials will depend upon discipline, methodology, and project specific considerations, as well as whether the primary materials are needed to substantiate the findings of the research, should those findings be contested. Where it is not practical or possible to retain certain primary materials (such as ore samples, biological material, or recordings) durable records derived from them (such as assays, test results, transcripts, and laboratory and field notes) should be retained and accessible.

7.6. Retention plans should be documented by the researcher in the DMP during data management planning (see section 3) and subsequently reviewed at:

a) completion of the data capturing phase of research

b) publication of research resulting from the data or of any data assets

c) end of the *minimum* recommended retention period

d) at any other time considered necessary by the researcher or the University.

7.7. Where the results from the research are challenged, or where research records may be relevant to research integrity allegations, all relevant data and primary materials must be retained until the matter is resolved.

7.8. If, after assessing all considerations in section 7.4 above, the data and primary materials are no longer required to be retained, researchers will obtain authorisation from their Head of Organisational Unit prior to disposing of research data or primary materials. Destruction of data classified as red must be arranged by Digital Research.

7.9. Researchers will keep documentation relating to the disposal of research data and primary materials, including the disposal process that was used, and will update any relevant metadata and DMP (or equivalent documentation) to include this information.

8. Sharing and reuse of research data

8.1. University researchers are encouraged to facilitate the sharing and reuse of research data in a responsible, ethical, and efficient manner in alignment with FAIR data principles. FAIR improves transparency, impact, collaboration, and innovation for the research community.

8.2. Additional consideration of CARE data principles are required for data related to Indigenous Peoples and marginalised communities to ensure data sharing or reuse is sensitive to the culture, concerns and priorities of these communities. This includes approaches that contribute to the collective benefit to the communities from which the data was sourced and so that community members have a say in how the data is used and disseminated.

8.3. In alignment with FAIR data principles, researchers are encouraged to publish any data products generated during their research projects, to maximise the impact, visibility, and utility of the research. Sharing of data may be required by funding bodies and publishers, for example the NHMRC's Open Access Policy and the ARC's Research Data Management requirements. Researchers will not unreasonably withhold University-owned research data and primary materials from use by other researchers unless required for ethical, privacy, legal, contractual or confidentiality reasons.

8.4. To ensure that the sharing and reuse of research data complies with ethical and legal obligations (such as privacy, cultural sensitivities and intellectual property rights) researchers should consider the following prior to sharing:

a) Ensure permission for sharing has been granted by any relevant data custodians or stakeholders and that a Data Sharing Agreement is in place if required.

b) Be aware of any legal restrictions on data sharing or reuse, including copyright, intellectual property rights, and contractual obligations and comply with relevant laws and regulations.

c) Apply appropriate deidentification techniques, such as anonymisation, transformation, or aggregation, to remove or mask personally identifiable or sensitive information in the dataset or ensure the data sharing methods including access controls are appropriate to the classification of the data being shared (see section 5).

d) Obtain informed consent from research participants, specifying the intended use and sharing of the data, and ensure that the data sharing and reuse practices align with the consent provided. Any variation will require ethics approval.

e) When transmitting data to third party platforms or cloud servers, such as utilising online generative AI tools, data should be deidentified and intellectual property, personal information or culturally sensitive information removed.

8.5. When publishing a dataset, researchers should:

a) Store and share data in established, trustworthy repositories that adhere to FAIR and CARE data principles, provide long-term data preservation, and ensure data accessibility.

b) Provide comprehensive metadata, following standardised vocabularies and schema, to facilitate the discovery, understanding, and reuse of the data.

c) Select an appropriate data license that clearly specifies the terms and conditions for accessing, reusing, and redistributing the data. Consider open licenses, such as Creative Commons or Open Data Commons, to promote data reuse.

d) Accompany shared data with thorough documentation, including methodology, data collection process, data processing steps, and any known limitations or biases.

e) Facilitate data discovery and citation by using unique identifiers such as Digital Object Identifiers (DOIs).

8.6. Researchers are encouraged to utilise the University's Research Data Portal for dataset publishing. The Research Data Portal securely stores datasets and allow researchers to make data findable through Research Data Australia's Search Portal. Researchers are to nominate the appropriate level of access to their data (open/mediated/closed) and select preferred Creative Commons licencing to ensure their rights as the data creator are protected.

8.7. Where there is a dispute concerning provision of access, the issue should be brought to the Head of Academic Unit and the data steward to resolve. If required, the issue can be elevated to the Deputy Vice-Chancellor (Research) or nominee to determine if the research data or primary materials will be made available, and the reasoning for the decision will be transparent and justifiable.

8.8. When reusing data, researchers should consider quality, attribution, ethical and legal compliance by:

a) Evaluating the quality and accuracy of the data, being aware of any potential biases, inconsistencies, or limitations in the original data collection and processing.

b) Properly acknowledging the original data source and its creators, following the terms specified in the data license, and citing the data using the assigned unique identifier (such as a DOI).

c) Ensuring that the reuse of data complies with relevant ethical guidelines and legal requirements, including data protection laws, copyright, and intellectual property rights.

9. Data breaches, loss or unauthorised access

9.1. Any data breaches, loss, or unauthorised access of research data must be reported in accordance with the University's *Cyber Security Controls Procedure*.

9.2. Where a breach or loss of data relates to:

a) Personal information, it will also be reported immediately to the University's Compliance Team (via email to databreach@utas.edu.au) in accordance with the *Data Breach Procedure.*

b) The deliverables associated with a research funding contract, it will also be reported to research.funding@utas.edu.au.

10. Research integrity and breaches of the Australian Code for the Responsible Conduct of Research

10.1. Research integrity concerns or breaches of the Code relating to research data management include, but are not limited to:

a) Falsification or fabrication of research data or primary materials.

b) Failure to notify the institution and relevant authorities in a timely manner of a data breach or instance of inappropriate access to research data.

c) Failure to retain clear, accurate, secure, and complete records of all research including research data and primary materials.

d) Failure to adhere to the conditions of any legal, institutional, or project-specific requirements relating to the retention, sharing or destruction of research data or primary materials.

e) Selective retention of research data or primary materials to hinder the verifiability of a research output or access request.

f) Failure to apply appropriate security controls to research data or primary materials.

g) Failure to obtain necessary approvals or acting inconsistently with a condition of any approval granted relating to the management of research data or primary materials.

10.2. Researchers are required to report non-compliance with this procedure to the Research Integrity Office in accordance with the *Research Integrity Complaints Procedure*.

Related procedures

Information Management Procedure

Cyber Security Controls Procedure

Research Integrity Complaints Procedure

Research Funding Costing Procedure

Collaborative Research Procedure

Research Integrity Complaints Procedure

Data Breach Procedure

Versions

Version	Action	Approved By	Business owner/s	Approval Date
1	Approved	Deputy Vice-Chancellor (Research)	Executive Director Research	10 November 2021
2	Approved	Deputy Vice-Chancellor (Research)	Executive Director Research Operations	10 November 2022
3	Approved	Deputy Vice-Chancellor (Research)	Executive Director Research Operations Associate Director Digital Research	8 November 2023
3	Reconfirmed, unchanged	Deputy Vice-Chancellor (Research)	Executive Director Research Operations Associate Director Digital Research	1 November 2024

Definitions

Research | Research data | University researchers

Schedule A: UTAS Data Classification Framework – Categories

	Green data refers to fully open data such as open access publications and external facing website content and should only be applied to data that has already been authorised for public access.
	Yellow data refers to information that has a more limited audience but where the loss or misuse of those data are unlikely to cause harm to an individual or institution. Examples of yellow research data include published datasets where data have been deidentified and appropriate licences have been applied, or data published in a gated access repository alongside sufficient metadata to define ownership and reuse criteria.
	Orange data has a restricted audience and loss or misuse of Orange data may have an adverse impact on an individual or institution. Most research data is classified as Orange by default due to containing a dimension of sensitivity (ie. personal, ecological, or cultural) or constraints such as contractual obligations, or intellectual property that requires protection.
	Red data has an extremely restricted audience. Loss or misuse of Red data is expected to result in serious harm to an individual or organisation and could constitute a criminal or regulatory offence. Red data may include unpublished research with extreme sensitivity or ethical implications as well as data or information subject to external classification regimes and other controls; for example, national security information, police records or information and primary materials subject to regulatory or export controls.

Schedule B: Resources and Advice

A. Advice is available to University researchers on all aspects of this procedure, with specific aspects and contact information provided below.

Digital Research: digital.research@utas.edu.au	University data storage options, data security, general data management support including instrument data, planning for future capability and data archiving
Research Funding Team: research.funding@utas.edu.au	Contractual agreements for third-party research data that is not in the public domain
Cyber Security: ict.security@utas.edu.au	Access controls, data security, data breach support
Research Integrity: research.integrity@utas.edu.au	Concerns or questions relating to research integrity or breaches of the Australian Code for the Responsible Conduct in Research
Human Research Ethics: human.ethics@utas.edu.au	Ethical issues relating to data for human research such as storage, destruction, confidentiality, and consent
Animal Research Ethics: animal.ethics@utas.edu.au	Ethical issues relating to data for animal research such as storage, destruction, confidentiality, and consent
Information Management Unit: imu.staff@utas.edu.au	Data retention, data and primary material archiving and disposal
University Library: utas.edu.au/library	Advice on data management, data publication, metadata and training
University Copyright: utas.copyright@utas.edu.au	Copyright obligations
Legal Services: Legal.Office@utas.edu.au	Intellectual property, privacy, Notifiable Data Breaches, and other legal obligations