Research Data Management Procedures

1. Purpose

1.1 The Research Data Management Procedures (the procedures) outline the mutual obligations of UTS and UTS researchers to ensure good data management practices in line with the Australian Code for the Responsible Conduct of Research (the Australian Code). The procedures should be read in conjunction with the Research Policy (the policy).

2. Scope

2.1 The procedures apply to all those under the scope of the policy.

3. Principles

3.1 The principles outlined in the policy apply for these procedures.

3.2 UTS communicates research methodology, data and findings openly, accurately and responsibly in line with the Management of Data and Information in Research (an Australian Code guide).

3.3 UTS is committed to open, equitable and worldwide access to its research in line with the Open Access Policy.

3.4 Researchers must take ethical and cultural considerations into account when collecting and managing research data.

3.5 Researchers will retain clear, accurate, secure and complete records of research, including research data and primary materials.

3.6 UTS will provide access to facilities for the safe and secure storage and management of research data and materials.

3.7 Researchers should apply discipline-appropriate processes in following these procedures.

4. Procedural statements

Planning a research project

4.1 Researchers should consider the type and volume of research data and materials they will be collecting and how it will be stored during and after the research project.

4.2 Where necessary, researchers should include costings for data management and storage in their research proposals.

Developing a research data management plan

4.3 Researchers must develop a research data management plan (RDMP) at the start of their research project. Research project leaders must ensure that a RDMP is completed and maintained for projects that they lead. At a minimum, the plan should address:

- the research project to which it is linked (title and/or MyProposal ID)
- the purposes for which the information will be collected, used and/ or disclosed
- the project's research project leader (lead chief investigator) and data manager
- where the data will be stored
- the size and form of the data
- who will have access to the data
- the data's security classification and how it will be protected
- the data's retention period and when it should be archived or destroyed
- sensitivities that apply to the data (commercial, privacy, ethical, security classification)
- what licence will be applied to the data.

4.4 RDMPs should be maintained over the lifetime of the project. An RDMP created in Stash will automatically cover the requirements of these procedures.

4.5 Once an RDMP has been created, researchers can use Stash to request research workspaces, which can be used to collect, store and analyse research data.

4.6 Researchers working with Indigenous peoples must reach an agreement regarding the storage of and access to data and determine strategies for allowing access and protecting confidentiality. Refer to 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.

4.7 A research project may extend beyond funding cycles and result in multiple research outputs. In these cases, it may be appropriate for researchers to create and maintain a single RDMP that outlines how they will collect, use and manage their research data.

Summary of responsibilities: Planning and developing a RDMP

UTS will	• provide guidance to researchers on how to manage their research data • provide tools and infrastructure to enable researchers to complete RDMPs.
Research project leaders will	• ensure that members of their projects are given appropriate training on research data management • ensure that an RDMP is completed and maintained for each project that they lead.

Researchers will	• complete and maintain RDMPs for their research projects • take ethical and cultural considerations into account when planning the collection and management of data.
Graduate research supervisors will	• ensure that their students are given appropriate training on research data management • ensure that their students complete an RDMP for their project.
Graduate research students will	• complete an RDMP for their project in consultation with their supervisors no later than their stage 1 assessment • nominate their chief supervisor as research project leader on their RDMP.

Working with data and materials

4.8 Researchers must store their data in research workspaces to:

- protect their data
- have a record of progress
- reduce the risk of accidental or deliberate deletion or falsification of data, and
- meet their research recordkeeping obligations.

4.9 Researchers working with primary materials, such as archival collections, must include management of these materials in their RDMP. They must consider how the materials can be preserved (for example conservation of objects, specimens and documents) so that they form part of the research data record. Where available, digital scans or images of the material should form part of the research data record.

4.10 Researchers working with primary materials should also consider how access to the materials may be granted to enable verification of findings and reuse if appropriate.

4.11 Primary research materials should be described with appropriate metadata (using recognised metadata standards where available), including enough information to allow an interested party to identify the materials. These metadata should be considered as research data and managed as such.

4.12 Researchers working with data for which they are not the copyright holder, such as archival materials or datasets supplied under licence by a third party, must ensure that they comply with the terms under which the data are supplied, including access, storage and publication.

Storage and classification

4.13 Research data should be stored on UTS owned or recommended infrastructure, as appropriate to the discipline and security classification of the data. Physical objects such as notebooks should be protected from loss or accidental disclosure.

4.14 Research data, especially sensitive data, should not be stored on portable storage devices such as external hard drives, laptops or phones, which may be lost or stolen. Data stored on a portable storage device must be encrypted to protect it from unauthorised access or use.

4.15 Researchers should refer to the UTS Information Security Classification Standard (PDF) available at Information Security (Staff Connect) for information on how to correctly classify their research data and determine where it may be stored. Refer Records Management Policy.

4.16 At a minimum, pre-publication research data will generally be classified as UTS Internal. Research data that contains personal information or is otherwise sensitive will have a higher security classification, which affects where it may be stored and how it must be protected. This includes physical copies of data that contain personal information, such as survey responses and interview recordings and transcripts.

Transborder data flows

4.17 UTS has personal and health information obligations under the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW) (HRIPA).

4.18 The NSW health privacy principle 14 (HRIPA, Schedule 1) states that health information about individuals should not be transferred outside New South Wales. Researchers working with individuals' health data must ensure that it does not leave the state, for example through use of cloud services that store or process data outside New South Wales. Storing data in line with statements 4.13 to 4.16 of these procedures will assist researchers in complying with this requirement.

Summary of responsibilities: Working with data and materials

UTS will	• provide guidance to researchers on how to store their data securely depending on its security classification • provide facilities to researchers to store their data appropriately for its security classification.
Research project leaders will	• apply the correct security classification to data from their project • store data from their project on appropriate infrastructure.
Researchers will	• understand the security classification that applies to their research data • understand the requirements that determine how their data must be stored • comply with data licences and agreements for third party data that they use • use appropriate infrastructure to store their data.
Graduate research supervisors will	• help their students to determine the correct security classification for their data • ensure that their students use the appropriate infrastructure to store their data.
Graduate research students will	• consult with their supervisors to determine the correct security classification for their data • use appropriate infrastructure to store their data.

Retention and disposal

4.19 Researchers must apply appropriate retention periods to their research data. The following are the usual minimum retention periods.

- Default period: Five years.
- Short-term projects: One year.
- Clinical trials: 15 years (may be longer if children or young people are involved).
- Gene therapy: Permanent.

4.20 Other retention periods may be specified by law, by the Human Research Ethics Committee or by a funding body.

4.21 The data manager must review the data at the end of the retention period. If the data are still in use, and there are no requirements to destroy the data, the data manager should nominate a further retention period for the data.

4.22 If destruction is required, discipline-appropriate processes must be followed, including for eResearch (Staff Connect) to securely delete any copies they hold.

4.23 If destruction is not required, the data manager may request that the data continue to be held in a data archive for a specified period or, in the case of data that has not been accessed and does not have associated publications, be deleted.

4.24 Datasets of significant community or heritage value should be assessed for transfer to a national archive or collection.

4.25 Researchers whose data are about Indigenous peoples should negotiate with the community regarding its retention and storage.

Leaving UTS

4.26 Researchers leaving UTS should ensure that their RDMPs are current and all their datasets have a specified retention period.

4.27 Data managers leaving UTS should review their datasets and arrange for another researcher, normally the research project leader or associate dean (research), to take on the role of data manager. In the case of a research project leader leaving UTS, the associate dean (research) or researcher taking over the research project leader role should be nominated as the data manager.

4.28 Subject to ethical, cultural, commercial and legal (including privacy) restrictions, researchers may take a copy of and/or continue to access their research data by entering into a data sharing arrangement with the data manager. This arrangement must be included in the research contract or in a separate data licence.

Summary of responsibilities: Retention and disposal and leaving UTS

UTS will	• provide guidance to researchers on how long data must be retained • provide facilities to researchers to archive their data • enable secure destruction of data once its retention period has expired.

Research project leaders will	• apply the correct retention period to data from their project • ensure that the nominated data manager for their projects is kept current.
Researchers will	• understand the requirements that determine how long their data must be preserved • apply the correct retention period to their data • make arrangements to transfer responsibility for management of their data to another data manager should they leave UTS • enter into a data sharing agreement with the data manager if they wish to take a copy of their data when leaving UTS.
Graduate research supervisors will	• help their students to apply the correct retention period to their data • help their students to create a data sharing agreement if required.
Graduate research students will	• consult with their supervisors to determine the retention period for their data • ensure that the correct retention period is applied to their data.

Access and rights

4.29 UTS subscribes to The FAIR Guiding Principles for scientific data management and stewardship, which act as a guide to increasing the reuse of research data. This is in line with the Open Access Policy.

4.30 UTS encourages researchers to open access to their data in line with the Australian Code's responsibilities of researchers 22, while recognising that they have the right to first use of their data (before publication).

4.31 Researchers should create data records for their datasets (and apply appropriate metadata). Publishing a data record that describes research data will help to make data more discoverable.

4.32 There are cases in which it is not appropriate for researchers to give open access to their data. These include but are not limited to the following.

- The researcher has been granted access to the data by a third party and is not licensed to share it.
- There are security reasons for not granting access to the data, including if the data contains information about the location of rare discoveries or threatened wildlife.
- The data are commercially sensitive.
- Research participants have not given their consent to the publication of data.
- The data contain personal and/or health information of participants and it cannot be effectively de-identified.
- The data relate to research with Indigenous peoples and they have not consented to release.

4.33 If researchers do not have consent to share identifiable research data, it may be possible to de-identify the data to enable sharing. However, de-identification of data are complex and re-identification may be possible in the context of other data. Researchers de-identifying personal information should consider the risks to

individuals should their data be re-identified prior to disseminating the de-identified data.

4.34 In some cases where open data publication is not appropriate, it may be possible for researchers to allow mediated access to interested parties. The data or a subset of the data may be supplied under a licence that restricts use and access to nominated people and projects.

4.35 Researchers should apply licences to their data that describe the conditions under which it may be accessed and used. Researchers should choose the least restrictive licence that is reasonable.

Archiving and publishing

4.36 Researchers should archive their research data in the UTS data archive. Archival copies of data may be deposited at regular intervals during the lifespan of a research project, which will help protect data against accidental or deliberate alteration or deletion.

4.37 Data records are created in Stash. The data will be linked to the relevant RDMP and will describe the data deposited in the data archive.

4.38 Some journals and funding bodies require researchers to publish their research data as part of research outputs. Publishing data enables it to be reused and cited by other researchers.

4.39 Researchers may choose to publish data via UTS's Research Data Portal. Some discipline-specific data repositories exist.

4.40 Data publication requests are generated via Stash and require a data record.

4.41 As part of publication, UTS will generate digital object identifiers (DOIs) for research datasets to support discovery and citation.

4.42 Researchers may choose to publish the data record in cases where it is not appropriate to publish the dataset.

Summary of responsibilities: Access, archiving and publishing

UTS will	• provide guidance to researchers on how to archive and publish data • provide facilities for researchers to archive and publish data.
Research project leaders will	• create a data record for data from their projects and archive the data • publish, where appropriate, data and/or relevant metadata to enable discovery of data.
Researchers will	• understand the archiving and publication requirements that are relevant to their data • create data records for their datasets, applying appropriate metadata • enable access to their data, either by publication or mediated access • apply appropriate licenses to their published data.
Graduate research supervisors will	• ensure that their students create a data record and deposit their data at the end of their project if appropriate,

Graduate research students will	• consult with their supervisors to determine how to archive their data and whether publication is appropriate • create a data record and archive their data at the end of their project if appropriate.

5. Procedure ownership and support

5.1 **Procedure owner:** The Deputy Vice-Chancellor (Research) is responsible for enforcement of these procedures, ensuring that its principles and statements are observed. The Deputy Vice-Chancellor (Research) is also responsible for approval of other associated university-level procedures and/or guidelines.

5.2 **Procedure contact**: The Manager, Research Integrity and Research Programs is the primary point of contact for advice on implementing and administering these procedures. The Manager, Research Integrity and Research Programs is also responsible for maintaining the official file, for proposing amendments as required and for managing the consultation process when the procedures are due for review.

5.3 **Others:** eResearch Manager is the primary point of contact for IT systems and storage advice in relation to research data management.

6. Definitions

The definitions outlined in the policy apply for these procedures. The following definitions are in addition to those definitions.

Data manager means the person who is the contact for all queries regarding the research data. It may be the researcher, a research assistant, a faculty data manager or a generic name and email (for example centre lab manager, centre@science.uts.edu.au). The person must be contactable after the end of the research project.

Data record means a description of a research dataset, created in Stash, that contains information on the contents and interpretation of the dataset. It also provides context on when and why the dataset was created, who can access it and how long it must be retained.

Dataset means a collection of related data, whether structured or unstructured, which has been collected or curated for a single purpose.

FAIR data principles are a set of principles that make research data findable, accessible, interoperable and reusable. The FAIR data principles are published as The FAIR Guiding Principles for scientific data management and stewardship.

Mediated access means access to research data (or related information) with the assistance of a UTS data manager or nominee and under specified conditions regarding use and dissemination.

Research workspaces are applications and services used to conduct research before data are exported for archiving. It includes but is not limited to storage and sharing platforms, collaboration services, survey and analytics platforms, code and project management, digital research notebooks and computing services.

Stash is the approved UTS system used to create research data management plans.

7. Approval information

Procedure contact	Manager, Research Integrity and Research Programs
Approval authority	Deputy Vice-Chancellor (Research)
Review date	Three years post approval
File number	UR20/1822
Superseded documents	Guidelines for the management of research data

Version history

Version	Approved by	Approval date	Effective date	Sections modified
1.0	Deputy Vice-Chancellor (Research)	04/12/2020	16/02/2021	New procedures.

8. References

AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research

Australian Code for Responsible Conduct of Research

Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders

Health Records and Information Privacy Act 2002 (NSW)

Management of Data and Information in Research (an Australian Code for the Responsible Conduct of Research guide).

Open Access Policy

Privacy and Personal Information Protection Act 1998 (NSW)

Research Data Portal

Records Management Policy

Research Policy and Procedures

The FAIR Guiding Principles for scientific data management and stewardship

UTS Information Security Classification Standard (PDF) available at Information Security (Staff Connect)