Research Data Management Policy process

Objective: This process sets out how researchers are expected to manage research data at RMIT. Researchers must ensure that their research data is managed in line with any requirements including ethics, legislation, contracts, and the provisions of the *Australian Code for the Responsible Conduct of Research* (the Code).

Scope

All researchers undertaking research at RMIT.

All research data that has been collected and/or used during RMIT research activities, including materials, raw and analysed data, research records and datasets, held in all formats and media.

Exclusions

Research management records, such as contractual materials, grant or funding applications, ethics approval material or other documents related to the management of research projects. These are managed in line with the **Privacy and Information Management Policy (unresolved)** and related processes.

Research outputs, for example journal articles and theses.

Definitions: [Will be put on a separate tab.]

The Australian Code for the Responsible Conduct of Research (the Code): Sets out good research principles and practices. It was developed by the National Health and Medical Research Council (NHMRC), the Australian Research Council (ARC) and Universities Australia.

Australian Privacy Principles (APP): Contained in the *Privacy Act 1988*. The principles regulate the handling of personal information by Australian government agencies and some private sector organisations.

Custodian: A person or organisation who is responsible for taking care of or protecting research data.

Databank: For human research this is data collected and stored for use in future research projects. For other types of research many terms may be used to describe a collection of data, including datastore, database and databank.

De-identify: Removing information which would allow the identification of the original source of the data.

Destruction: Eliminating or deleting records, documents or information, beyond any possible reconstruction.

Disposal: Disposal can include retention, the transfer of ownership or custody (e.g. to an archive or repository), deletion or destruction of data.

Metadata: Information about research data that enables it to be identified, retrieved and re-used. Important metadata elements may include subject matter, collectors and owners, and technical or contextual information that enables the data to be understood.

Research data: Research data are the material, data, records, files, and other evidence upon which a research project's observations, findings, or outcomes are based.

This includes all content and forms (e.g. print, digital, physical or other forms), and both primary material and analysed data.

Examples of research data are laboratory notebooks, survey forms, specimens, computer code and any other records needed to reconstruct or evaluate reported results of research, and the events and methods leading to those results.

Secondary data: Data that was not collected specifically for the research project, data that was collected by other people for another project or purpose.

Introduction

RMIT University values the contribution of researchers and participants to the collection of research data. We recognise the importance of research data in supporting research findings, contributing to further research and discussion, and enabling public trust in research.

It is important that research data are managed well throughout the data lifecycle, to respect any legal requirements and confidentiality, ethics and privacy concerns; and so that the data are secure and reusable.

What is research data management?

It is organising the collection, analysis, storage, description and disposal of research data. It ensures that researchers and institutions are able to meet their obligations to funders, improve the efficiency of research, and make data available to verify their findings or for reuse, where appropriate.

What are research data?

Research data are the material, data, records, files, and other evidence upon which a research project's observations, findings, or outcomes are based.

This includes all content and forms (e.g. print, digital, physical or other forms), and both primary material and analysed data.

Examples of research data are laboratory notebooks, survey forms, specimens, computer code and any other records needed to reconstruct or evaluate reported results of research, and the events and methods leading to those results.

Who has responsibilities for research data management at RMIT?

This process sets out researchers' responsibilities. However, research data management extends across an institution. The Research data management responsibilities diagram (PDF 121KB 1p) shows how responsibility is assigned at RMIT.

Process steps:

1. Recording research data management

1.1. For each research project, record how the research data that is collected and/or used will be managed. Include the following information:

- Describe the research data (include the format, type and quantity of data);
- Where the data is stored and how it is secured (see Section 4);

- Who has access to the research data and how access is controlled (see Section 7);
- If the data will be made discoverable and accessible to other researchers, and how this will be enabled (see Section 8);
- Any restrictions on access or reuse (see Section 7);
- Any confidentiality requirements;
- Who owns the research data and related Intellectual Property and Copyright (see Section 3);
- How long the research data will be kept for (see Section 10);
- How the research data will be archived, disposed of or destroyed, and who will do it (see Section 12 and 13).

1.2. Keep this record up to date during and after the research project. See RMIT's Research Data Management Library Guide for more information and resources that you can use to record, store and manage research data.

1.3. Share this record with others involved in the research and/or your supervisor/s.

2. Managing research data

2.1. Be aware of the people and areas at RMIT involved in research data management and their responsibilities. See Research data management responsibilities diagram (PDF 121KB 1p).

2.2. Use infrastructure provided or approved by RMIT to manage research data, where possible. Where you do not, ensure that any provisions and/or terms of service associated with external infrastructure comply with RMIT policy and any other requirements.

2.3. When collecting or using confidential, personal, sensitive or health information where people could be identified, follow any ethics requirements and RMIT's **Privacy and Information Management Policy (unresolved)**.

2.4. Ensure that all people collecting or handling research data:

- Are appropriately qualified to do so, and,
- Are aware of any ethics or contractual requirements, relevant policy and legislation.
- This includes other researchers and people providing support, for example translation, transcription, data analysis, and image processing.

3. Ownership

3.1. Record who owns the research data collected and used during the research project. See RMIT's Copyright Checklist for Research Data Management.

3.2. Follow any conditions on data handling and use due to ownership. When using research data from third parties follow any reuse conditions (see Section 3.3). Make a record of these conditions (see Section 1.1).

3.3. Follow any Intellectual Property law, legislative requirements or guidelines that apply to the research data. For more information see RMIT's **Intellectual Property Policy (unresolved)**.

3.4. Storing research data on RMIT infrastructure does not affect ownership.

4. Storage

4.1. Store research data so that it is safe, secure, durable, indexed, easily retrievable and accessible; and so that it complies with legal, ethics, and *Code* requirements and discipline norms. For more information see RMIT's Library Guide for Storing Research Data and ITS webpage on Storing Research Data.

4.2. Do not store research data only on Google Applications or personal storage devices (PSDs). Only use PSD's temporarily and when necessary, because they may be lost, stolen or damaged. Never store confidential, personal or sensitive information on a PSD unless it is encrypted.

4.3. Store confidential, personal and sensitive research data securely:

- Do not store it on Google Applications.
- Encrypt this data if it is stored on a portable storage device (PSD) - such as USB keys, laptops or compact disks.
- Follow the RMIT **PSD Use and Security Process (unresolved)**.

4.4. Use the storage space provided by your school for non-electronic research data, where possible.

4.5. Store electronic research data on RMIT infrastructure or storage solutions approved by RMIT, where possible. See the ITS webpage for information on research data storage options.

4.6. You may digitise hardcopy research data and keep the digital version instead of the hardcopy version. You can digitise data, for example by scanning or photographing the data. The digital version of the data must be a full and accurate digital replication, stored in a durable and accessible format (e.g. pdf), and indexed.

5. Data banking

5.1. When collecting research data about people, their information or their tissue for a databank, researchers must gain consent in line with Chapter 2.2 of the *National Statement on Ethical Conduct in Human Research*. Contact the Human Research Ethics Coordinator for advice. Human research ethics approval is also required.

5.2. A databank must have a named custodian. The custodian ensures that the data are used responsibly and safeguards participants' privacy.

6. Moving research data

6.1. When moving data across state or national borders, follow any relevant legislation or ethics requirements, including the privacy principles on trans and cross border data flows (See the Health Privacy Principle 9 (PDF) and the Australian Privacy Principle 8).

6.2. When importing or exporting any research material, follow relevant legislation and regulations and obtain any necessary permits. Contact your school for advice, and see also the Australian Quarantine Inspection Service regulations, and RMIT's Sanctions and Defence Trade Controls webpages.

6.3. Use RMIT approved cloud systems to to move data where possible, for example Cloudstor.

6.4. When moving research data between RMIT and any other institutions, have a documented agreement that covers research data retention, ownership, and access. This should be agreed between all of the institutions and the Chief Investigator(s) and/or the Dean/Head of School.

6.5. If leaving RMIT University:

- You may remove any research data that you own, provided a copy of the data remains accessible to RMIT for the minimum retention period.
- You may take copies of research data from your research projects, subject to legal, confidentiality, contractual, ethics and other requirements.
- Update your research management arrangements. Share this information with your supervisor and/or other people involved the research. Issues to review include data ownership and user conditions, access agreements, custodian arrangements for databanks, retention requirements and data disposal.
- Students conducting research should leave a copy of their research data prior to graduation.

6.6. When you move research data, update records with the new location of the data and any related changes, such as access arrangements. Notify the Chief Investigator that the data has been moved. This includes if you move data within RMIT (see Section 1.1).

7. Access and re-use

7.1. During and after the research project, the Chief Investigator, or the person responsible for the data, controls access to the data and any reuse of the data. Record the people who have access to the data, and the access and reuse conditions.

7.2. Make sure that access to and/or reuse of research data complies with:

- confidentiality requirements,
- cultural issues,
- commercial interests,
- reuse permissions,
- legal requirements including intellectual property rights, and,
- privacy and ethical considerations and requirements.

Key issues to consider are the type of consent granted, and whether the data should be identifiable, re-identifiable or non-identifiable.

7.3. Protect confidential or sensitive research data from unauthorised access. If you are given access to confidential data, maintain its confidentiality.

7.4. Research data, even confidential data, may be accessed by subpoena in the event of legal action and in certain other circumstances under the *Freedom of Information Act 1982* (VIC).

7.5. Contact the school for clear information about discipline specific reuse permissions, terms, and conditions in relation to research data management.

8. Making research data discoverable

8.1. Make research data available to other researchers and support reuse of research data, where possible. When you cannot make the research data available, make the research metadata available.

8.1.1. Contact the Library for advice on how to describe the data, how to clean the data, and on the appropriate data storage facility, archive, repository or metadata store to use.

8.1.2. See Section 11.1 of this Process for how to store data so it can be referenced or reused.

8.1.3. Researchers with funding will need to follow any funding body guidelines on data management. The National Health and Medical Research Council (NHMRC) and Australian Research Council (ARC) encourage researchers to share and reuse data arising from research projects in publicly accessible repositories, where possible.

9. Retention

9.1. Retain relevant research data, during and after the research project. Generally, research data must be kept for a minimum of 5 years from the date of publication. The following considerations affect what data you have to keep, and the retention period (see Section 10) and method (see Section 11):

- You may have keep all of the research data, for example it may be a condition of ethics approval;
- Keep enough research data to verify both the outcomes of the research and to defend them if they are challenged;
- You may want to reuse or share the research data;
- Journals, other researchers and interested parties may want to reference the data that supports the research findings.
- The value of the research data and discipline norms; and,
- Legislative, contractual and regulatory requirements.

9.2. You do not have to keep secondary data, but do keep a reference of where and when you accessed the secondary data. You do need to keep the data analysis.

9.3. You may not have to retain research materials and raw data (such as ore, biological material, questionnaires or recordings) where it is impractical due to issues such as size, but you must keep sufficient related process data (such as test results, transcripts, diary entries, lab books and notes) to capture the relevant information about the data and how it was collected and analysed. This may include documentation of oral decisions and commitments related to the research data.

10. Retention period

10.1. Keep research data for at least the minimum retention period.

10.2. In most cases, this means keeping research data for five years from the date of publication. Some research data has different minimum retention periods, as follows:

Type of research data	Minimum retention period

Most research data	At least 5 years
Short-term research projects conducted for internal assessment (e.g. student research projects)	12 months from the end of the project
Health information	7 years
Clinical research, including clinical trials	15 years or more
Areas such as gene therapy	Permanently
Work that has community or heritage value	Permanently, preferably within a national collection

For more information on retention periods see RMIT's Research Data and Record Retention Factsheet. Minimum retention periods are in line with the Higher Education Records Disposal Authority issued by the Public Records Office Victoria (under Section 12 of the Public Records Act 1973), the *Health Records Act 2001* (Vic), the Code.

10.3. Where the research data has multiple retention periods, keep the data for the longer retention period.

10.4. You can keep research data for longer than the retention period, unless there is a requirement to dispose of the data, for example if it is a condition of ethics approval.

11. Retention method

11.1. Enable long term preservation and description of the research data, as follows:

- Index the research data;
- Use durable formats to store data (such as csv files or pdfs);
- Agree file format types prior to data collection;
- Clearly state access and reuse permissions, terms, and conditions; and,
- Record this information, for example, on RMIT's Research Data Catalogue.

11.2. Keep electronic research data on infrastructure provided or approved by ITS. If not, ensure that the provider's terms of service comply with RMIT policy. See ITS webpage on research data storage for more information.

11.3. Retain hardcopy research data in the school or in an appropriate data repository, data management facility, or professional association. Record where it is located.

11.4. You may retain copies of the research data collected during their research activities at RMIT University for your own use, subject to RMIT's **Intellectual Property Policy (unresolved)** and any legislative, ethics, contract, or confidentiality requirements.

11.5. Contact your school for information about:

- Which research materials, raw data and hardcopy data to retain.
- Appropriate facilities for their retention.
- How long the data should be kept.

12. Disposal

12.1. You may dispose of your data by transferring ownership or custody (e.g. to an archive or repository), deleting it or destroying it.

12.2. Before disposing of research data, consider whether there are any reasons to keep the research data (see Section 9) and ensure the research data has been retained for at least the minimum retention period (See Section 10). For destruction see Section 13.

12.3. Dispose of research data appropriately, in line with relevant legislation and guidelines, statutory requirements, funding and contractual requirements. Disposal must be as secure and as environmentally friendly as possible.

12.4. You may dispose of copies of research data at any time without permission. Where necessary, dispose of the copies securely.

12.5. Deposit research data in an appropriate repository that is publicly accessible, where possible.

13. Destruction

13.1. You may need to destroy research data, for example, due to ethics conditions, legislative requirements or contractual agreements. Before destroying data consider the value of the data, if it could be used for further research, or if it is still required to support the research findings.

13.2. Before destroying research data, get approval from the data owner (where the data is not owned by RMIT University); or the Dean/Head of School and/or relevant researcher(s) responsible for managing the data.

13.3. Do not destroy research data that are relevant to complaints about research practice, allegations of breach of the Code or research misconduct, court proceedings or Freedom of Information requests until the matter is fully resolved.

13.4. Use irreversible methods to destroy research data so that the data are no longer readable or usable, and cannot be recreated. Take extra care when the data are sensitive or confidential.

- To fully delete digital data, you may need software that permanently erases data. Contact Information Technology Services for advice and support.
- Destroy non-digital data appropriately, for example, shred it, use secure document disposal bins. Do not destroy hardcopy research data using ordinary waste or recycle bins.

Related policy: Research Policy

Supporting documents: Research data management library guide

Research data management responsibilities diagram (PDF 121KB 1p)

Cross-referenced to:

Feedback link: Policy@rmit.edu.au

Custodian/s title and email:	Executive Director, Research Office	Custodian email	researchintegrity@rmit.edu.au
Date approved:	5 September 2016	Last approved:	1 August 2017
Responsible unit/s:	Research Office (Research Integrity, Governance and Systems)	Published/effective date:	29 September 2016
Review date:		Document ref:	POL/2018/00024[V2]