DISCOVERY & INNOVATION UNIT

PROCEDURE

RESEARCH DATA MANAGEMENT PROCEDURE

Staff this document applies to:

- All Austin Health staff including honoraries
- All visitors involved in research associated with, or supported by Austin Health, including fellows, scholars and students

Related Legalisation & Austin Health policies, procedures or guidelines:

- Copyright Act 1968 (Cth)
- Defence Trade Controls Act 2012 (Cth)
- Electronic Transactions Act 1999 (Cth)
- Health Records Act 2001 (Vic)
- Privacy Act 1988 (Cth)
- Public Record Act 1973 (Vic)
- National health Security Act 2007 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Conflict of Interest Policy
- Code of Conduct Policy
- Fraud, Corruption Control and Other Losses Policy
- Gifts, Benefits and Hospitality Policy
- Patient Safety and clinical excellence framework
- Radiation Safety Policy
- Research Authorship and Outputs Procedure
- Research Misconduct Procedure
- Research Policy

Key points:

- **Part A:** Roles and responsibilities
- **Part B:** Research data planning
- **Part C:** Storage of research data and primary materials
- **Part D:** Ownership, responsibility and control
- **Part E:** Retention and disposal of research data
- **Part F:** Safety and security
- **Part G:** Access and transfer of research data and primary materials
- **Part H:** Sharing research data
- **Part I:** Exit planning
- **Part J:** Disposal of research data and primary materials
- **Part K:** Framework for research data
- **Part L:** Definitions

OPPIC Document ID: PRC-23387 **Date of last major update: 2/09/2024** **Review Date:** 02/09/2027

Scope

This procedure applies to:

(1) Research data and records generated during research undertaken by Austin Health Staff and students who may or may not have a University or Medical Research Institute affiliation.

(2) Research data and records in any form, including digital formats, paper formats and other physical materials.

(3) This procedure does **not** apply to research where responsibility for data has been allocated to a third party through a written agreement.

Purpose

The objective of this procedure is to:

(4) Preserve the value of research data and records for researchers, research students, research participants, the Hospital, its Research Partners and wider community by defining expected standards for data.

(5) Facility effective research practices in the management of research data, all primary materials and research recordkeeping.

(6) Encourage researchers to publish research data in formats that meet disciplinary standards, as well as being in line with the F.A.I.R principles, which means data must be finable, accessible, interoperable and reusable.

Part A – Roles and Responsibilities

(7) Austin Health is responsible for maintaining a governance framework for research data management as outlined in this procedure. This responsibility has been delegated to the Discovery & Innovation Unit who will oversee the direction and implementation of research data management across Austin Health.

(8) Austin Health is responsible for:

a. Establishing and communicating processes to manage research data and research records in accordance with Public Record Act 1973 (Vic), or as determined by other statutory requirements, funding agency guidelines or contractual arrangements with research partners.

b. Providing or securing approved facilities for the safe and secure collect and storage of research data and primary materials, and research recordkeeping.

c. Ensuring backup, archival and monitoring processes are in place to prevent loss of research data and primary materials.

d. Providing a mechanism to make research data available for use by other researchers except where the sharing of data is prevented by privacy, confidentiality or other ethical, contractual or legal obligations.

e. Providing training, support, advice and guidelines that promote a best-practice approach toward Research Data Management.

f. Monitoring compliance of researchers with applicable policies, legislation, ethical or contractual obligations.

(9) Austin Health Departments or Units, or other organisational units (or equivalent) are responsible for:

a. Providing storage facilitates in their departments/units for physical research data and primary materials to meet security, confidentiality and safety requirements and maintaining clear and accurate records that help to locate and retrieve stored data and materials.

b. Ensuring their researchers and research students are aware of their responsibilities for research data and primary materials.

(10) Chief Investigators (CI) are responsible for:

a. Considering the management of research data and primary materials issues at the earliest point of a research project, and documenting decisions made for the creation, storage, sharing and retention of research data and primary materials.

b. Allocating appropriate resources (time, personnel and financial resources) for data management in any related grant proposal.

c. Identifying and establishing the storage requirements of their research data and primary materials throughout various stages of the research lifecycle and managing data in accordance with this procedure and Austin Health IT Security Policy.

d. Ensuring research personnel collecting or handling research data are appropriately qualified and aware of their responsibility to comply with Austin Health policy, ethical and legal requirements.

e. Reporting any breach of security or confidentiality to their Head of Department/Unit, Chief Information Officer, and/or relevant ethics or biosafety committee as appropriate.

f. Ensuring research data are formatted and stored in a manner that renders it open to scrutiny and review and available for reuse during the data retention period for the research project. Sufficient data should be retained to allow justifications of research findings.

(11) Austin Health Researchers are responsible for:

a. Ensuring data are accurate, complete, authentic and reliable.

b. Keeping clear and accurate records of research methods, data sources, approvals granted during and after the research process.

c. Applying best-practice data management practices processes in research projects to comply with this procedure and relevant privacy legalisation.

d. Ensuring research data and primary materials are retained for as long as they are of continuing value or interest to the global research community, or other interested parties as specified by any research funding agreement, professional standards, legal or other requirements.

(12) Supervisors of students enrolled in a research degree are responsible for:

a. Applying the same procedural principles outlined above in (9) and (10) for students with the exception that all responsibilities are jointly held by research students and their supervisors.

b. Supervisors must provide guidance and mentorship to research students on appropriate management of research data and records for their field of research, in line with their host organisation's relevant research training/student policies.

c. Research students and supervisors must agree on the management of research data and records at the start of a research project, including plans for how research data and record will be managed following thesis submission. The Discovery & Innovation Unit recommends these arrangements be outlined in the approved protocol but can also be outlined in a Data Management Plan.

(13) Researchers and Austin Health are jointly responsible for ensuring that research data and records are:

a. Accurate, complete and authentic and supports verification of research results

b. Compliant with ethical and legal obligations

c. Identifiable, retrievable and available with minimal barriers

d. Secure from loss and degradation.

(14) Failure to comply with this procedure may:

a. Lead to researchers or Austin Health being held legally responsible for breaches of legislation.

b. Be considered a breach under the Australian Code for the Responsible Conduct of Research and be investigated in line with Austin Health's Research Misconduct Policy which aligns with the NHMRC Guide to Managing and Investigating Potential Breaches of the Australian Code for the Responsible Conduct of Research.

c. Be handled in line with Austin Health Code of Conduct Policy and other relevant policies and procedures.

Part B – Research data planning

(15) All new research proposals must include a Research Data Management Plan (RDMP), that clearly documents research data management issues, such as the collection, ownership, retention, export or supply, storage and preservation of research data and primary materials. At a minimum, documentation must address what data is to be generated by the research and the plans for managing the data. Austin Health recommends that this management plan is embedded within the protocol. If this information cannot be included in the protocol, a separate Research Data Management Plan is to be included in the ethical and legal review of the project.

(16) Research data and primary materials must be collected and managed in accordance with best practice standards within research fields and disciplines, as well as meeting legal, statutory and ethical requirements.

(17) Research involving human participants, materials, samples or data requires approval from a Human Research Ethics Committee (HREC) or Institutional Review Board in accordance with Austin Health Research Policy and relevant terms of reference.

(18) When research is conducted across multiple organisations, agreement should be reached in writing which clearly specifies the principles of control, storage, transfer and retention of research data within each organisation.

(19) When sourcing secondary data from parties within or outside Austin health the CIs must ensure they have the required permissions to use the materials as part of their project. All licence agreements or permissions should be submitted to the Discovery & Innovation Unit, who where appropriate, will triage any requests to General Counsel to ensure terms and conditions granted by rights holders meet the legal/licencing requirements of the research project.

(20) Confidential information and personal information must be managed in accordance with Austin Health's privacy policies, contractual obligations, and ethical approval requirements for each project.

(21) If conducting research involving Indigenous people CIs must:

a. Apply the Australian Institute of Aboriginal and Torres Strait Islander Studies (AIASIS) Code of Ethics for Aboriginal and Torres Strait Islander Research (2020) and the NHMRC Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities (2018) and NHMRC Keeping research on track II (2018) or any equivalent guidelines in local jurisdictions when formulating a research data management plan; and

b. Consult with research participants and communities regarding the methods of collecting, storing and accessing the data.

c. Provide access to Indigenous data owners to uphold Indigenous Culture and Intellectual property rights. Access should be given in line with Australian Institute of Aboriginal and Torres Strait Islander Studies (AIASIS) Code of Ethics for Aboriginal and Torres Strait Islander Research (2020) and the NHMRC Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities (2018) and NHMRC Keeping research on track II (2018).

(22) Research involving the use of animals, including observational research, requires approval from the Animal Ethics Committee (AEC) in accordance with Austin Health Research Policy and relevant terms of reference.

(23) Research involving gene technology, genetically modified organisms (GMOs) or microorganisms classified as Risk Group 2 or higher requires approval from the Austin Health Institutional Biosafety Committee in accordance with Austin Health Research Policy and relevant terms of reference.

Part C – Storage of research data and primary materials

(24) CI, researchers, student supervisors and student researchers must ensure research data and primary materials are stored securely in a durable and accessible form.

(25) In the active research phase, CI must maintain clear and accurate records of where their research data and primary materials are stored. Record keeping must provide sufficient information to identify the location, attribution, ethical approvals, access provisions and terms of use of the data. Changes or developments in the project, such as moving working research data into long-term storage, must be updated in the project's protocol and/or affiliated research data management plan.

(26) Researchers must regularly back-up all original materials collected or organised on portable devices onto approved storage system. Personal, confidential or sensitive data that is being held or transferred on a portable storage device should be encrypted to prevent unauthorised access to data.

(27) Generally, research data and primary materials must be retained for sufficient time to allow reference to them by other researchers and for as long as interest and discussion persist following publication.

(28) Data deemed to be of ongoing value to the research community, and required for the potential defence of the veracity of the data or its analysis must be retained in an approved archive, repository, or other storage infrastructure.

a. Digital research data that underpins published or reported findings must be deposited into approved research data portal or other approved facility.

b. Non-digital data (e.g. materials, samples, printed materials, pre-digital recordings) should be retained in the research unit in which they were generated or other approved facility.

(29) Digital and physical curation to ensure research data remains available for re-use must be applied when research data and primary materials move from the active research stage into preservation and long-term storage.

(30) At the point of publication research data and primary materials must be evaluated in accordance with any contractual or other legal or ethical requirements about that data to determine what must be retained and what can be disposed of.

(31) When identifying research data and primary materials for preservation, CIs should consider the potential value of the materials for future research, especially where the research would be difficult or expensive to repeat. Sufficient research data and primary materials must be retained to justify the outcomes of research and, if necessary, to defend them against challenge.

(32) To preserve the value and investment made in research, the data must be well organised, clearly labelled, and saved in durable file formats that will support long term preservation of the materials.

(33) Researchers must create clear and accurate records whereby the research data and primary materials can be discovered and retrieved by an authorised person other than the researcher. The records must include:

a. The location of data and primary materials

b. The location of physical keys, passwords, or other devices necessary to access

c. Information on indexes, catalogues or other finding tools necessary to access the

d. Conditions of access.

(34) At the end of a research project, research data and primary materials relating to outputs must be appraised, archived and assessed for retention in perpetuity unless there are conditions (such as ethics approvals, contractual obligations, or legislative requirements) which mandate that the data and materials are destroyed at the end of the project.

Part D – Ownership, responsibility and control

(35) Researchers must ensure that ownership of and responsibility for research data and records is identified and documented at the start of a research project, ideally in the approved protocol/project description, by exception in a separate data management plan. Data management must be approved by the relevant ethics or institutional review board committee/s, depending on type of project and data. Data management should be reviewed and updated as appropriate with consideration given to:

a. Authority to decide on storage, retention, disposal, publication or licensing of research data or records

b. Research data ownership as outlined by the Austin Health Intellectual Property Policy, or by the relevant University, Medical Research Institute or Sponsor Intellectual Property declared prior to approval of the research project at Austin Health

c. Agreements with funders, data providers, research partners and collaborators

d. Arrangements for researchers changing institutions or withdrawing from collaborative projects; and

e. Any Indigenous Cultural and Intellectual property rights , for research involving Aboriginal and Torres Strait Islander peoples (in line with Australian Institute of Aboriginal and Torres Strait Islander Studies (AIASIS) Code of Ethics for Aboriginal and Torres Strait Islander Research (2020) and the NHMRC Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities (2018) and NHMRC Keeping research on track II (2018).

(36) Researchers must ensure that Austin Health has a record of ownership and responsibility for any research data and records they have transferred into or out of Austin Health. With relevant approvals in place, Austin Health will approve for data to be managed and stored outside of Austin Health, if data management, security and storage are outlined in the protocol/research data management plan and in relevant research agreements.

(37) In the event no ownership or responsibility has been recorded, or the recorded responsible party is no longer an Austin Health researcher, the Research Director or delegate will hold authority to decide on storage, retention, disposal, publication or licensing arrangements in compliance with legal and regulatory obligations.

Part E– Retention and disposal of research data

(38) Researchers must curate and store accurate, complete and authentic research data and records in formats that are understandable, retrievable and accessible to appropriate parties.

(39) Metadata should be stored with research data and records to support interpretation, authenticity and reproducibility.

(40) Where it is not practical to store physical research data and records, durable records documenting or derived from them should be stored in digital formats.

(41) When not using Austin Health provided facilities, researchers must ensure that processes and facilities used for storage and management of research data and records comply with ethical and legal obligations. Where researchers are unsure of their ethical and legal obligations, they should consult with the Discovery & Innovation Unit at Austin Health.

(42) Researchers must ensure that research data and records are retained and disposed of in line with minimum retention periods specified in their ethics and/or legal approvals.

(43) Researchers are encouraged to deposit research data and records into approved facilities at the conclusion of research activity/project, to support the retention obligations. Where research data and records are already stored in Austin Health facilities, researchers must ensure that the research activity's completion is recorded in Austin Health's research management system to allow for appropriate retention and disposal.

Part F – Safety and security

(44) Researchers must ensure the safe and secure management of research data and records to comply with ethical and legal obligations over the life of the research data and records, with consideration given to research data and records with sensitivities, including:

a. Personal information subject to privacy legalisation, including information that may be considered personal information when linked with other information

b. Sensitive cultural information e.g., on sacred cultural practices

c. Information subject to export controls, as regulated by the Defence Trade Control Act (2012)

d. Information on security sensitive biological agendas (SSBAs) as regulated by the National Health Security Act (2007)

e. Commercial in confidence information.

(45) Researchers should document plans for the safe and secure management of research data and records to ensure all authorised individuals with access follow documented plans. These plans ideally should be outlined in relevant approved protocols/project description.

(46) Researchers must ensure that research data and records are transferred and stored with electronic or physical security controls to restrict access to authorised individuals. Controls must be appropriate to the level of sensitivity as defined within this procedure.

(47) Austin Health must ensure that facilities provided for the storage and management of research data and records meet legal and technical requirements in line with Austin Health Data Classification Framework contained within this procedure and the Austin Health Information Security Policy.

(48) Researchers must manage personal and health information in line with Austin Health Privacy Policy and processes outlined in the Research Policy.

Part G – Access and transfer of research data and primary materials

(49) Access to research data and primary materials must be controlled by appropriate security measures to prevent unauthorized access and comply with any agreements in place relating to confidentiality, consent or commercial interests.

(50) Where there is a dispute concerning the provision of access to research data or primary materials, the Discovery & Innovation Unit and General Counsel must be consulted. On the advice of General Counsel, the Clinical Director of Research or nominee will determine whether the research data or primary materials should be made available.

(51) In situations where access to data is governed by an agreement with a third party, access to the data will be handled on a case-by-case basis upon advice from the General Counsel.

(52) All research data intended to be transferred outside of Australia must be assessed by the CI to determine if the transfer of the research data is affected by export control laws. All permit applications must be sought through Austin Health registered personnel, and records of transfers must be maintained for the approved duration period by the CI. Records must be made available to Austin Health upon request.

Part H – Sharing research data

(53) Research data must be made available for re-use or re-purposing where possible, subject to privacy, ethical, contractual or legal limitations that prevent the sharing of data.

(54) Electronic research data is to be deposited in an appropriate public repository in accordance with any contractual obligations required by funding bodies or publishers.

(55) All research data affected by defence export control legislation must comply with the requirements for exporting, supplying, publishing and brokering.

(56) Where ethical or legal limitations apply, researchers should consider if meditated access or sharing of a limited subset is possible.

(57) When making research data or records available to interested parties, consideration should be given to:

a. Data ownership, including intellectual property rights, Indigenous Cultural and Intellectual property rights.

b. Agreements with funders, research partners, data providers and publishers

c. Meeting ethical and legal obligations such as preserving privacy, intended use and consent for use of data at the time of collection

d. Ensuring safety and security through agreements with interested parties that define required controls.

(58) Researchers must make available any research data and records substantiating research findings to enable academic discussion or evaluation of research outputs, unless prevented by ethical or legal obligations. Where research data or records have been requested and access refused, the reasons must be transparent and justifiable.

(59) Researchers are encouraged to publish research data and records to disciplinary, institutional or other repositories to allow reuse by other researchers and maximise the value of research, unless prevented by ethical or legal obligations.

(60) Researchers should consider applying the least restrictive licensing option that is appropriate for governing the future use of their published research data.

Part I– Exit planning

(61) Researchers leaving Austin Health should ensure that a copy of their research data and records has been deposited into Austin Health facilities to support research integrity and retention obligations, as consistent with ethical, contractual or legislative requirements.

(62) When a research leaves Austin Health they must ensure custodianship of their data is transferred to an appropriate researcher as determined by the Head of Division/Unit. All original data must remain at Austin Health, unless otherwise agreed via a formal agreement between Austin Health and the new host organisation.

Part J – Disposal of research data and primary materials

(63) Research data and primary materials, and registers of those materials, are Austin Health records. When the specified period of retention has finished, they must be disposed of in a secure and safe manner in accordance with the Code, the Austin Health Records and Archives Management Policy, and the Victorian Public Records Act.

Part K – Framework for research data

The Framework for Research Data Classification will help you make informed decisions about your sensitive data management. The Framework distils regulatory requirements and best-practice cybersecurity standards into a simple and actionable format. It represents Austin Health's endorsed recommendations for assessing and managing your sensitive research data. The Framework classifies research data into four categories ranging from 'Green' (least sensitive) to 'Red' (most sensitive), based on the potential severity of harm to subjects, researchers, or Austin Health in the event of disclosure or access by unauthorised parties.

Descriptions and examples of each classification level are provided in the table below as a general guide.

Classification level descriptions

Data Classification	Description
Green	The green classification applies to information that presents the risk of **negligible** material, social, reputational, legal, or other harm to individuals, communities, or organisations in the event of accidental or unauthorised access, disclosure, alteration, misuse, loss, or destruction. **Examples:** • Information intended for public disclosure / consumption • Published manuscripts or datasets • Data from public websites or social media that does not relate to an identified or identifiable individual
Yellow	The yellow classification applies to information that presents the risk of only **limited** material, social, reputational, legal, or other harm to individuals, communities, or organisations in the event of accidental or unauthorised access, disclosure, alteration, misuse, loss, or destruction. **Examples:** • De-identified or aggregated data that does not relate to an identifiable individual or present any risk of significant harm to a community or group • Unpublished research data and outputs that do not fall into all other categories, e.g., drafts of research publications, novel creative works etc. • Novel analyses or transformations of publicly available data or information

	• Data generated by instruments, imaging systems or computational models that are not linked to a specific identifiable entity
Orange	The orange classification applies to information that presents the risk of **significant** material, social, reputational, legal, or other harm to individuals, communities, or organisations in the event of accidental or unauthorised access, disclosure, alteration, misuse, loss, or destruction. **Examples:** • Personally identifiable data including name, contact details, financial details, individual medical records, etc. • Genetic or biometric information • Re-identifiable data i.e., when the identity of a specific individual or other sensitive entity can be reasonably ascertained by data linkage or other activities • Culturally sensitive data
Red	The red classification applies to information that presents the risk of **severe** social, psychological, reputational, financial, legal, or other harm to individuals, communities, or organisations in the event of accidental or unauthorised access, disclosure, alteration, misuse, loss, or destruction. **Examples:** • Personally identifiable data containing "sensitive" information as defined by Victorian Privacy legislation • Assets and information for defence research, or that have the potential to be adapted for military or 'dual use' applications • Data involving Sensitive Security Biological Agents (SSBAs)

The Classification Framework focusses predominantly on Australian legislative requirements and is not comprehensive of all legal, ethical, and regulatory instruments that may impact your research. You must abide by any ethical or contractual requirements you have in place.

Part L – Definitions

Accessible means that access to research data and records by interested parties is enabled through defined processes. These processes may include authentication and authorisation steps to restrict or mediate access to appropriate parties.

Authentic means that research data and records are a true and accurate product or reflection of research processes with no attempts to falsify, mislead or obfuscate.

Curate means to select, organise and present information in ways that support interpretation. Appropriate curation of research data and records is informed by accepted disciplinary practices and standards and will differ depending on the type of research data and records involved.

Data management plan means a plan that is embedded in the protocol/project description, by exception it can be a separate document that outlines how research data and records will be managed through the course of a research project, including details such as project descriptions, software and systems being used, storage locations, security controls, retention and disposal arrangements.

Facilities means physical or virtual locations intended for a defined purpose. For the storage and management of research data and records, this may consist of a combination of physical space, equipment, hardware, software and the resources required to support these.

Findable means the research data or records are discoverable to interested and authorised parties for reuse. Characteristics of findable research data or records include assigning metadata that describes the content of the research data or records, attaching a persistent identifier such as a Digital Object Identifier (DOI) and indexing/making the data searchable through disciplinary portals.

Interested parties means any parties who are seeking access to research data this may be for the purposes of academic review, ethical or compliance review, or data reuse for further research.

Interoperable means that the research data or records can be effectively integrated with other data or be utilised by different applications or workflows (such as for analysis, storage or processing). To achieve this, community-agreed, published standards are used within and to describe the research data and records.

Mediated access means access that is determined on a case-by-case basis by an individual responsible for the data, who is able to assess the value and risk associated with data sharing.

Metadata means information that provides contextual details or defining characteristics about data. Meaningful metadata is dependent on the type of research data it is describing, allowing data to be interpreted accurately and appropriately. Metadata may describe, for example, where the data originated, how the data was generated and processed, when the data was collected and by whom.

Ownership means the legal or moral rights that gives individuals, groups or organisations the authority to determine storage, retention, disposal, publication or licensing arrangements.

Personal information means any information regarding an individual whose identity can be ascertained from that information.

Research data means any information, facts or observations that have been collected, recorded or used during the research process for the purpose of substantiating research findings. Research data may exist in digital, analogue or combined forms and such data may be numerical, descriptive or visual, raw or processed, analysed or unanalysed, experimental, observational or machine generated. Examples of research data include, but are not limited to: documents, spreadsheets, audio and video recordings, transcripts, databases, images, field notebooks, diaries, process journals, artworks, compositions, laboratory notebooks, algorithms, scripts, survey responses and questionnaires.

Research record means documents containing information of any kind and in any form created or received by an organisation or person for use in the course of their research. Records often validate the provenance, authenticity and ethical collection of research data. Records associated with the research process include correspondence, grant applications, ethics applications, authorship agreements, technical reports, research reports, laboratory notebooks or research journals, master lists, signed consent forms, and information sheets for research participants.

Research student means is any student involved in conducting research using Austin Health patient, staff or other data/biospemens collected under the auspices of Austin Health. This includes graduate researchers and coursework students and visiting students enrolled at any institution.

Researcher means any individual involved in conducting research at Austin Health who is not a research student. This includes staff, honorary staff and visiting researchers.

Retention means the long-term storage of research data and records after the completion of a research activity/project, for the purposes of meeting legal obligations or other purposes.

Reusable means being able to be utilised by others for replication of research findings or additional research applications, such as linkage with other data. This can be achieved by having standard data usage licences, provenance information and the use of domain-relevant community standards used throughout the research data and records.

Document author/contributors:

Author: Heidi Gaulke, Operations Director, Discovery & Innovation Unit

Contributor(s): James Best, Clinical Director of Research

Legislation/references/supporting documents:

- NHMRC Australian Code for the Responsible Conduct of Research (2018)
- NHMRC Authorship Guide
- NHMRC Publication and dissemination of research guide
- Australian Institute of Aboriginal and Torres Strait Islander Studies (AIATSIS) Code of Ethics for Aboriginal and Torres Strait Islander Research (2020)

- NHMRC Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and Communities (2018)
- NHMRC Keeping research on track II (2018).

Endorsed by:

Research Steering Committee

Document Owner /Person Responsible for Document:

Heidi Gaulke, Operations Director, Discovery & Innovation Unit

OPPIC Document ID: PRC-23387 **Date of last major update:** 01/03/2023 **Review Date:** 01/03/2026