Cairnmillar INSTITUTE

Treatment | Education | Research

Research Data Policy

391-393 Tooronga Road Hawthorn East Vic 3123 T: 9813 3400 www.cairnmillar.edu.au

Policy number	RP005
Date approved	1 April 2020
Approving body	Academic Board
Responsible officer	Head of School
Implementation officer	Associate Head of School Research
Next review date	April 2023
Linked policies	Research Conduct Policy Human Research Ethics Policy
Linked forms	Release of Confidential Information Form Human Research Ethics Committee Application Form

Purpose

This policy outlines the Cairnmillar Institute's (the Institute) policy for the responsible conduct of research, specifically relating to the collection, use, disclosure, storage, retention, disposal, dissemination and re-use of research data and related information. This policy is in compliance with the Australian Code for the Responsible Conduct of Research, 2018 (the Code).

Scope

This policy applies to all research undertaken by staff and students of the Institute.

Policy

Data management

a) All researchers must develop a research data management plan which covers the following aspects of a research project: data collection, ownership, storage, access, retention and disposal.

b) All researchers must adhere to all relevant ethical, intellectual property and confidentiality agreements when developing the research data management plan.

Data collection

c) The principal investigator is responsible for data collection and management of any resulting information from the research project.

d) All researchers must keep accurate and detailed records of research data and materials in order to justify research outcomes, provide evidence, if required, of ethical recording of data and defend the research findings if challenged. This includes any approvals or amendments granted during the research process.

Data ownership

e) Data ownership is to be identified, discussed and agreed upon at the start of a research project. Any changes or amendments to data ownership is to be updated and reviewed whenever appropriate.

f) Ownership of research data and any related research materials will be construed under the Institute's Intellectual Property Policy and procedures.

g) Confidentiality agreements may be negotiated between the institute, the researcher and any person or body funding the research.

Data retention and storage

h) Research data and related materials must be retained for a minimum of five years. Although research data may be retained for longer periods, such retention must not breach any ethics conditions or approvals given prior to the collection and retention of the research data.

i) Research data must be securely stored for a minimum retention period of five years to protect research data from theft, loss, damage or misuse. Data must be kept in a retrievable form. Secure storage means on a secured share drive or in a locked cabinet, or equivalent, in a secure location.

j) Any additional professional body, funding body or contractual arrangement for the security and protection of research data must be adhered to by researchers, where it is agreed in writing.

k) If research staff or research students leave the Institute during the data retention period, if agreed in writing, a copy of the material or data may be

transferred to a new secure storage location for the research individual's use for the duration of the retention period.

Data access

l) Researchers who have access to confidential information and research data will maintain confidentiality in accordance with all ethical, privacy and contractual conditions, including agreements with the research participants.

m) Researchers are responsible to ensure that appropriate security is in place to protect any confidential material, but also providing appropriate access to all researchers.

n) Researchers must report any privacy or storage breach in relation to research data to the Chair of the Research and Research Training Committee.

Data disposal

o) The principal investigator is responsible for disposal of research data and materials.

p) Disposal must be undertaken after the appropriate retention period and must be done in compliance with appropriate privacy considerations, such as shredding personal information to ensure data cannot be accessed by unauthorised persons or used in an unauthorised manner.