Research Data Management Guidelines

Section 1 - Purpose

(1) This guideline supports the Research Data Management Procedure by providing additional information and guidance for the management of research data at Charles Sturt University (the University).

Scope

(2) These guidelines have the same scope as the Research Policy.

Section 2 - Policy

(3) These guidelines support the Research Policy.

Section 3 - Procedure

(4) These guidelines support the Research Data Management Procedure.

Section 4 - Guidelines

Research data management plans (RDMP)

(5) Research data management plans (RDMP) are prepared for all research projects, in accordance with the Research Data Management Procedure.

(6) The Office of the Deputy Vice-Chancellor and Vice-President (Research) maintains the register of RDMPs.

(7) RDMPs are submitted as an accompanying document with applications submitted to any of the following committees, in accordance with the terms of reference and submission processes of those committees:

a. Animal Care and Ethics Committee
b. Human Research Ethics Committee
c. Institutional Biosafety Committee
d. Radiation Safety Committee

(8) Research students, in consultation with their research supervisor(s), must create and register an RDMP prior to the commencement of a research project.

(9) The RDMP should be reviewed regularly, either annually or as changes arise, to ensure it accurately reflects the research project at any given time. Research students review their RDMP in consultation with their research supervisor.

(10) RDMP planning should adhere, to the extent possible, to the findable, accessible, interoperable, and reusable

(FAIR) data principles.

Data Storage and formats

Storage

(11) The nature of the research data collected will dictate the appropriate storage solution to use.

(12) Information about University managed storage options is available in the Library's guide to Research Data Management at Charles Sturt: Store and Manage. Researchers should be aware of the data storage requirements for specific funding agencies and ethics approvals.

(13) Storage options must take into consideration the data security requirements, set out below.

(14) Physical data that cannot be digitised can be stored at the CSU Regional Archives.

(15) Physical data other than paper (non-standard formats for example) must be stored appropriately and ensure compliance with the University's workplace, health and safety and other policies and procedures.

(16) If storage of non-standard formats is not possible within the University, it may be necessary for researchers to gain written approval from the Pro Vice-Chancellor Research (Performance and Governance) to approach external third parties for storage options.

Formats

(17) Researchers must ensure the longevity of research data by choosing formats that are durable, indexed and retrievable for the duration of the retention period, or longer if required. Some of the digital formats are text, images, audio, videos, spatial data, CAD files, databases and websites.

(18) Research data should be managed and be made accessible as it is required, regardless of the file format or the technology used when they were originally created.

(19) NSW State Records provides a list of recommended file formats best suited for long-term sustainability and accessibility.

(20) Wherever possible and appropriate, physical research data, primary materials and research records should be digitised in a preferred format, to minimise the risk of loss or damage, and minimise physical storage requirements.

a. Physical data should be converted into a durable format if possible, quality checked for any errors and completeness, and then stored digitally.
b. After physical data has been converted to digital form, the original physical data can be destroyed once the minimum retention period for source documents has been met, and in accordance with the Records Management Procedure.

> Note: Examples of digitisation include scanning documentation, manuscripts or participant consent forms to PDF format; or photographing physical materials and storing them in TIFF format.

Retention, archiving and disposal of data

(21) Retention of research data is required for all projects but in particular where the data is critical to the substantiation of research findings and cannot be readily or practically duplicated and for research that is:

a. controversial or of high public interest, or has influence in the research domain

b. costly or impossible to reproduce or substitute if the primary data is not available (e.g. cannot be substituted with an alternative data set of acceptable quality and useability, or if data reproduction would place unnecessary burden on human research participants or animals), or
c. relates to the use of an innovative technique for the first time.

(22) Minimum retention requirements for University owned research data are set out in the following table. These comply with the requirements of the NHMRC guidelines and State Records Act. Longer retention periods may be required by contracts with third-parties (e.g. publisher agreements, grants).

Data Set Type	Retention Requirements
Data and datasets created as part of research activities which do not involve clinical trials, research with potential long term effects on humans, gene therapy or which are not of regulatory or community significance.	5 years after project completed
Data and datasets created from clinical trials, or research with potential long term effects on humans, as part of research activities within the institution, which are not of regulatory or community significance. Includes animal testing for human products.	15 years after completion of research activity or until subject reaches or would have reached the age of 25 years, whichever is longer
Data that is: 1. part of genetic research, including gene therapy 2. controversial or of high public interest, or has influence in the research domain 3. costly or impossible to reproduce or substitute (i.e. with an alternative data set of acceptable quality and useability) if the primary data is not available, or 4. related to the use of an innovative technique for the first time	Retain permanently, State Archive

(23) Researchers must ensure that all research data owned by the University and sufficient metadata is made available to the University within 12 months of completing the research activity so that retention periods can be managed.

(24) the University, at its absolute discretion, may determine to keep the research data beyond the minimum period. Where this occurs, restricted data must be de-identified and any confidential or personal information removed.

(25) The CSU Regional Archives, as a regional archives centre, will maintain custody of the research data required as a State archive and facilitate access where appropriate, whilst control of the research data will pass to NSW State Archives and Records Authority.

Data security and confidentiality

(26) Secure storage of University owned research data must, at minimum:

a. allow setting up access and permission controls to protect records from unauthorised use, alteration, deletion or removal (such as user registration/deregistration)
b. have security controls that allow logging, monitoring and termination of access and use. The logs should be protected from tampering.

(27) Most University managed systems will support these requirements.

(28) Where a storage system does not support the requirements, the RDMP should include details about how the security of the research data will be managed.

(29) Research data that includes personal or sensitive information, or that is classified as highly confidential or confidential/private under the University's data security classification scheme may be subject to higher than the minimum security requirements. See the Privacy Management Plan and Information Security Guidelines for further information.

(30) As per the Research Data Management Procedure, storage of University owned research data outside of University managed systems and facilities require approval and should include information about how security requirements will be met.

(31) There are various data protection techniques available including password protection on files and folders, encryption, de-identification, saving in ‘read-only’ formats and keeping portable storage devices locked away when not in use.

Section 5 - Glossary

(32) This procedure uses terms defined in the Research Policy and Research Data Management Procedure.

Status and Details

Status	Current
Effective Date	8th December 2023
Review Date	8th December 2026
Approval Authority	Deputy Vice-Chancellor (Research)
Approval Date	8th December 2023
Expiry Date	Not Applicable
Unit Head	Mark Evans Deputy Vice-Chancellor (Research)
Author	Tracey Kerr Policy Developer
Enquiries Contact	Office of Research Services +61 2 69332578