



University of
Salford
MANCHESTER

Research Data Management Policy

Version Number 2.1

Effective from 1 September 2026

Author: Academic Support Manager (Research)

The Library, Careers & Skills

1.0 Purpose

This policy outlines the University of Salford's requirements for research data management before, during, and after a research project's lifecycle. The University champions good practice in research data management because it is integral to high-quality research and aligns with funder requirements and the values and priorities set out in the [University of Salford Strategy 2026-2030 Innovating to Enrich Lives](#).

Active management, secure storage and retention, and timely deletion of research data are necessary for research integrity, information security, and environmental sustainability. Making research data as open as possible and only as restricted as necessary is important to the University's commitment to openness in research, supporting reproducibility and maximising the potential for re-use and impact.

This policy is supported by, and should be read in conjunction with, the [Research Data Management Guidance](#) published on the Library's webpages.

2.0 Scope

This policy applies to all research activities involving the collection, analysis, and storage of digital and physical research data conducted by University staff, postgraduate research students enrolled on a research degree, visiting or emeritus staff, associates, holders of honorary and clinical contracts, contractors and consultants and others working on the University premises or carrying out research activity in the name, or on behalf of the University of Salford, and across all subject disciplines and fields of study, hereafter referred to as 'Researchers'.

The policy does not apply to postgraduate taught students or undergraduates, but best research practice is recommended, and support and guidance is available to everyone.

3.0 Definitions

Term	Definition
Creative Commons Zero (CC0) licence	A Public Domain, No Rights Reserved licence with which creators and owners of copyright- or database-protected content waive those interests in their works so that others may freely build upon, enhance and reuse the works for any purposes without restriction under copyright or database law. See: https://creativecommons.org/public-domain/cc0/
Data management plan	A formal document that describes how research data will be collected, organised, stored, secured, backed-up, preserved, and where applicable, shared.
Data steward	A person employed in any role by the University of Salford who is identified by the researchers as being responsible for the management of a specific set of research data for the purposes of continuity. The choice of data steward will depend on the nature of the research project and project team. For example, the data stewardship role may be undertaken by a senior researcher, data curator, project officer, research technician, or the supervisor of a research student.
FAIR Principles	FAIR data are data which meet principles of findability, accessibility, interoperability, and reusability.

Metadata	Metadata is the data that provides information about other data. This can include the source, format and location of the other data. Metadata enables the discovery and reuse of other data, and can be administrative, descriptive, or technical.
Personal Data	The University adheres to the Information Commissioner's Office (ICO) definitions of personal data .
Principal Investigator (PI)	Principal Investigator (PI): Within this Policy, "Principal Investigator (PI)" means the staff member or student primarily tasked with conducting the research project at the University of Salford, whether or not they are referred to as such in a research grant. For external collaborative projects, this would be the lead researcher based at the University of Salford.
Research	The University of Salford adheres to the Frascati definition of Research as described in the Research Code of Practice.
Research data	The University defines research data as 'information created, observed or collected in the course of research which is necessary to support or validate a research project's observations, findings or outputs'. Research data may take physical or digital form.
Research data management	Research data management involves activities throughout the research data lifecycle; planning and making decisions about the collection, protection, organisation, storage, preservation, publishing and sharing of research data.
Researchers	Researchers refers to all University staff, postgraduate research students enrolled on a research degree, visiting or emeritus staff, associates, holders of honorary and clinical contracts, contractors and consultants and others working on the University premises or carrying out research activity in the name, or on behalf of the University of Salford, and across all subject disciplines and fields of study.
Sensitive data	'Sensitive data' is used as a catch-all term to refer to: • research data containing personal identifying information, 'personal data' and special category data as defined in UK data protection legislation; • commercially sensitive data, including data generated or used under a restrictive commercial research funding agreement; • data relating to species of plants or animals where the release of data may adversely affect rare or endangered species; • data likely to harm an individual or community or have a significant negative public impact if released. Sensitive data may also be classified as confidential according to the University's Information Security Policy.

4.0 Policy statements

Researchers' responsibilities:

4.1 Compliance

All researchers are responsible for following their funders' and the University's policies for research data management (RDM), in particular the University of Salford Data Protection Policy, Information Security Policy and ICT Acceptable Use Policy, Research Security Policy, and Academic Ethics Policy. All researchers are responsible for managing their

research data in accordance with contractual, legislative, regulatory, ethical, and other specified requirements and as set out in the project's Data Management Plan (see 4.3).

4.2 Accountability

The lead researcher (Principal Investigator or equivalent) on a research project is primarily accountable for RDM practices within the project. They must ensure that all research data are generated, stored, managed, and shared in accordance with contractual, legislative, regulatory, ethical, and other specified requirements, including any funder policies.

- 4.2.1. The lead researcher must ensure that, where external partners are involved, research data ownership is established and confirmed contractually in advance of a research project starting, in accordance with the University's Intellectual Property Policy and relevant third-party agreements. They must ensure that any access to research data by third parties is managed in accordance with the Information Security Policy.
- 4.2.2. Postgraduate research students are primarily responsible for RDM practices within their project. Supervisors of research students are responsible for ensuring that their students are aware of, and conduct research in accordance with the Research Code of Practice and all related University policies and external legislation, and are adequately trained and have a clear understanding of RDM requirements and appropriate practice.
- 4.2.3. RDM responsibilities can be shared or delegated but should be clearly documented in a Data Management Plan, and the lead researcher retains overall accountability. If leaving the University they must nominate a data steward, recorded in the Data Management Plan, to ensure the ongoing management, retention, and timely destruction of research data.

4.3 Data Management Plans

The lead researcher must ensure a Data Management Plan (DMP) is created for every research project which sets out how research data will be collected, classified, protected, prepared, securely stored, retained, and, wherever possible, shared.

- 4.3.1 The DMP must be created before the beginning of the research project, typically at the funding application or ethical approval stage.
- 4.3.2 DMPs are living documents which must be reviewed and kept up to date throughout the project. Researchers should use standardised DMP templates wherever possible.
- 4.3.3 All members of the research project team must be aware of, and abide by, the DMP.

4.4 Protecting sensitive data

Researchers must protect sensitive data and the rights of research participants in accordance with legislation, contractual agreements, and ethical requirements.

- 4.4.1. Sensitive and confidential research data can be shared ethically and legally when this has been planned and agreed before collection, following relevant professional, ethical and discipline-specific standards. These include, but are not limited to, gaining informed consent from participants; protecting identities through anonymisation or pseudonymisation; and controlling access to data where necessary

- 4.4.2. Where data will be shared with internationally-based collaborators and/or partners, including third-party, it is the lead researcher's responsibility to ensure any and all research security expectations (including licences) are in place before any data is shared outside the UK.

4.5 Costs

Researchers must plan for the resources required to store, retain, and manage their research data throughout the data lifecycle.

- 4.5.1. When preparing a research funding application, researchers must include all appropriate costs related to research data. This includes, but is not limited to, costs for research data storage, long term retention, and the digitisation of any physical data.
- 4.5.2. Researchers must identify their data storage requirements at the outset. If these needs exceed the standard storage allowance provided by the University, researchers should contact Digital IT and suitable arrangements should be made to cover any additional costs.

4.6 Storage during the project

While in active use, researchers must ensure that research data are stored safely, securely and protected from loss using facilities appropriate to the data medium.

- 4.6.1. Researchers must store digital research data on secure digital systems with a back-up mechanism to protect against loss. Where, due to the circumstances of data collection, research data needs to be temporarily stored on mobile devices or external storage, data classified as confidential must be encrypted and in all cases researchers must ensure data security in line with the Information Security policy.
- 4.6.2. The loss of sensitive data or University IT equipment must be reported according to the ICT Acceptable Use Policy.

4.7 Retention

Researchers are responsible for selecting which research data to retain by considering potential long-term value, reproducibility of the research findings, and legal or funder requirements. Selected research data must be retained for at least any period stipulated by legal, contractual, regulatory, or ethical requirements, and in line with discipline-specific norms, typically at least 10 years from publication.

4.8 Disposal of data

Researchers, or research data stewards, must securely dispose of research data identified for deletion or destruction with particular concern for the confidentiality and security of the data, in accordance with legal, contractual, regulatory, or ethical requirements and the University's Information Security Policy.

4.9 Depositing research data

Researchers must deposit their selected research data in an appropriate data repository as soon as possible. Access to deposited data can be restricted where necessary. Researchers may choose to use either:

- **The University's Research Data Repository (Figshare)** or

- **A suitable third-party data repository** which complies with legal, regulatory, and ethical requirements and aligns with FAIR principles to ensure data are Findable, Accessible, Interoperable, Reusable.

- 4.8.1. Where research data are deposited in a repository other than the University's Research Data Repository, researchers must enter a metadata record into the University of Salford Institutional Repository (USIR).
- 4.8.2. Where research data selected for retention are not in digital format, they should be digitised where possible. Where digitisation is not possible, researchers should seek to store the data in facilities appropriate to the subject matter and medium. To ensure these data are discoverable, a metadata record should be added to the University of Salford Institutional Repository (USIR).

4.10 Preparation of data

Researchers are responsible for preparing data prior to deposit and/or sharing. Before depositing research data, researchers must ensure that any sensitive data are prepared and protected in accordance with the consent given by participants, and any legal, contractual, regulatory, or ethical requirements (see 4.4).

- 4.10.1. Research data held or registered in any repository or data registry must be accompanied by metadata that clearly describe the data in sufficient detail to allow other researchers to find and understand them.
- 4.10.2. Where research data have been made openly accessible, they should be accompanied by sufficient descriptive and technical metadata and documentation to enable reading, reuse, and interoperation by humans and machines.

4.11 Data sharing

Research data selected for deposit must be made as open as possible and only as restricted as necessary. To enable open data sharing and maximise reuse and reproducibility, researchers should choose the most permissive Creative Commons licence possible (e.g. CC 0 licence). Researchers should minimise the time period for which they hold exclusive use of the data, as permitted by ethical, legislative, regulatory, commercial, and contractual conditions.

4.12 Data underpinning publications

A data access statement describing where supporting data can be found and accessed must be included in the publication when mandated by the research funder or publisher, even where the study generated no original research data, or the data are restricted or otherwise not accessible. In all other cases, a data access statement is strongly encouraged. Research data that underpins published research findings should, where possible, be made openly available at the time of first online publication.

4.13 Data underpinning theses

Where postgraduate research students have created or collected original research data which underpins the findings of their research, and these are not included in the thesis itself, they should ensure that selected data is stored in accordance with this policy. Research students are strongly encouraged to add a data access statement to the thesis. This statement should describe where supporting data can be found and accessed, even where the data are restricted or otherwise not accessible. Guidance is set out in the PGR Code of Practice.

University responsibilities:**4.14 Research data storage services and repositories**

The University will provide digital research data storage services and an open research data repository which comply with legal, regulatory, ethical, and information security requirements.

4.14.1 Research data deposited in the University's open research data repository will be retained for the length of time detailed in the data management plan.

4.14.2 . Where research data selected for long-term retention are not in digital format and cannot be digitised, the University will support researchers to identify facilities and resources required for preservation within the data management plan.

4.15 Guidance, training and support

The University will provide support, guidance and training for researchers, including supervisors of research students, to enable effective research data management throughout the research lifecycle.

5.0 Policy Enforcement and Monitoring

Breach of this policy will be considered as having the potential to bring the University and its employees into disrepute and managed in that context. Specific processes will be brought to bear in this context, including the Research Misconduct Policy and Procedure, the Academic Misconduct Procedure, and the Disciplinary Policy.

Periodic monitoring against this policy will be undertaken by The Library and Research and Knowledge Exchange (RKE) and be reported to the Research Enterprise & Innovation Committee (REIC).

6.0 Related Documentation

Internal Websites (the Hub)
Academics Ethics Staff website
Academic Handbook
Academic Regulations for Research Awards
Code of Practice for the Conduct of Postgraduate Research Degree Programmes
Concordat to Support Research Integrity
Information Governance website
Quality Management Office
Research Data Management
Research Policy
Senate and Committees website
Student Facing Procedures website
Policies and Procedures (all internal)
Academic Ethics Policy
Academic Misconduct Procedure
Data depositor agreement
Data Protection Policy
Disciplinary Policy
ICT Acceptable Use Policy
Information Security Policy
Intellectual Property Policy
Research Misconduct Policy and Procedure
Records Retention Schedule
Research Code of Practice

Safeguarding Guidance for Research
Scheme of Academic Governance
University Ethics Framework
Terms of Reference
Academic Ethics & Research Integrity Committee
Governance, Nominations, and Ethics Committee
Research, Enterprise & Innovation Committee
School Ethics Approval Committee
School Research, Enterprise and Engagement Ethics Approval Panel
Related external legislation, policies and information
Data Protection Act (2018)
National Security in Research Policy
Go FAIR – FAIR Data Principles

7.0 Contact

- a. Queries regarding research data management and open research should be directed to library-research@salford.ac.uk.
- b. Queries regarding research policies should be directed to research-governance@salford.ac.uk.
- c. Queries regarding digital systems, services or software should be directed to Digital IT [Service Portal](#)

Document Control Information			
Revision History incl. Authorisation: (most recent first)			
Author	Summary of changes	Version	Authorised & Date
T Williamson & Jack Brook	<i>Minor amendments to provide clarification based on feedback from the Research Data Management Working Group and Research Governance. Updates to job titles. 4.2.2 Bringing supervisor and student responsibilities in line with the Research Code of Practice 4.3 Numbering. Introduced recommendation for use of standard DMP template. 4.4.2. Inserted new statement outlining research security requirements. 4.5 Clarifying language around costing requirements. 4.9 Clarify deposit and repository options. 4.10 Introduced 'or registered' to account for data which is recorded in a data repository or registry 4.14 Disposal moved to 4.8 after Retention for clarity. 4.15 (now 4.14) Disambiguate repositories and storage services Updates to links and contact information</i>	V2.1	Research & Enterprise Committee: 20/05/2026
E Smith & T Williamson	<i>Significant rewrite. Restructured to reflect research lifecycle. Scope and definitions clarified; related policies section expanded and updated. Added explicit reference to physical data. Updated statements relating to information security. 12-month data deposit deadline removed. Added reference to FAIR data principles. Added recommendations re use of CC0 licenses for data and inclusion of data access statements in publications and theses.</i>	V2.0	Research & Enterprise Committee: 10/06/2024
H Baker & D Clay	<i>New policy</i>	V1.0	Research & Enterprise Committee: 04/11/15
Policy Management and Responsibilities:			
Owner:	This Policy is issued by the Pro-Vice Chancellor Research & Enterprise, who has the authority to issue and communicate policy on research data management and has delegated day to day management and communication of the policy to The Library. All subjects of the Policy will be responsible for engaging with and adhering to this policy.		
Others with responsibilities (please specify):			
Author to complete formal assessment with the following advisory teams:			
Equality Analysis (E&D, HR) Equality Assessment form	1. <i>Approved February 2024. Ref EIA2024-22</i> 2. <i>Reviewed by Director of Legal Services, May 2024.</i>		
Legal implications (LPG)			

Document Control Information	
Information Governance (LPG)	3. <i>Reviewed by DIT information security team and Director of Legal Services, May 2024.</i>
Student facing procedures (QEO)	4. <i>N/A</i>
UKVI Compliance (Student Admin)	5. <i>N/A</i>
Consultation:	
Staff Trades Unions via HR	1. <i>N/A</i>
Students via USSU	2. <i>N/A (PGR Forum consulted, including PGR student representation)</i>
Relevant external bodies (specify)	3. <i>N/A</i>
Review:	
Review due:	2 years by May 2028
Document location (webpage):	Library Research Data Management web page. RKE
Document location (link)	https://www.salford.ac.uk/library/open-research/open-data/research-data-management
The owner and author are responsible for publicising this policy document.	