University of Lancashire

Research Data Management Policy

Document type	Policy
Document owner	Research and Knowledge Exchange Service
Approved by	Open Research Steering Group – 28 November 2025 University Research and Innovation Committee – 21 January 2026
Approval date	21 January 2026
Review date	January 2029
Version	Version 4.1 (Approved January 2026)
	Amended July 2019; September 2019; October 2025
Summary of changes	• Inclusion of information on how researchers can fulfil their data management obligations (2.0). • References added to the Concordat on Open Research Data and various otherprocedures since the last version (3.0). • Updated to reflect FAIR principles, integration of DMPOnline, updated PGR responsibilities, GDPR compliance, and repository name change to Lancashire Online Research Data (formerly UCLanData) (4.1).

This document is available in alternative formats on request via the Open Research Team

Research Data Management Policy

1. Introduction and purpose

In reference to institutional research policies, it is useful to define what constitutes research. The University of Lancashire defines research in line with the Frascati Manual definition of research and experimental development[1] and in accordance with the Research Excellence Framework (REF 2029) definition, which states that "research is a process of investigation leading to new insights, effectively shared".

As an institution, the University of Lancashire fully supports open research and open practice. Research data generated at the University is recognised as an institutional asset that when shared openly not only increases the visibility of the University of Lancashire's research but also facilitates public engagement and creates new opportunities for knowledge exchange and collaboration.

In order to be made open access, research data must be created and managed with sharing in mind at every stage of the research process, from planning to publication.

This Research Data Management Policy clarifies the University's expectations concerning the management, storage, publication and sharing of research data. This Policy reflects the University's intention to establish good research data management practice throughout the research lifecycle as part of the institution's commitment to research excellence. The policy provides a strategic framework for the management and governance of research data generated by research activities at the University of Lancashire and aims to contribute to readiness for future Research Excellence Framework exercise or similar requirements.

This policy is underpinned by the FAIR Data Principles[1] (Findable, Accessible, Interoperable, and Reusable). The University is committed to ensuring research data are managed 'as open as possible, as closed as necessary' to balance openness with ethical and legal considerations.

2. Purpose of the research data management policy

- Ensure the University and its research communities are compliant with current academic and funder requirements such as the UK Research and Innovation (UKRI) Common Principles on Data Policy, the Wellcome Trust Policy on Data Management and Sharing, Horizon Europe Open Data Software and Code Guidelines, the REF 2029 Open Access Policy, and the Concordat on Open Research Data.
- By requiring deposit of key datasets, to ensure the widest possible audience for research data assets produced at the University of Lancashire in order to facilitate discovery, citation, sharing and collaboration and thereby to increase impact
- Clarify responsibilities so that researchers understand exactly what is required of them

[1] FAIR Principles - GO FAIR

- Contribute towards a culture of openness and transparency
- Establish data deposit as an integral part of the open access process
- Ensure the concept of data sharing is built into the research process from planning to publishing
- Ensure key datasets are preserved and accessible for as long as required by funder, ethics committee or the University
- Set out the University's obligations including the provision of facilities for the archiving of research data, training, support and guidance on good practice in research data management
- Draw attention to existing relevant documentation that underpins and clarifies elements of the policy with particular regard to obligations of a legal, ethical, regulatory and contractual nature

3. Scope of policy

This Policy applies to all University of Lancashire staff, honorary and visiting researchers, and postgraduate research students (PGRs) involved in research activity. PGRs, in consultation with their supervisory team, should use appropriate tools for data management planning, storage and deposit, including the University supported DMPOnline and Lancashire Online Research Data[2] repository.

4. Policy Awareness

All researchers should familiarise themselves with relevant University of Lancashire policies, in particular this Research Data Management Policy, the Open Access Policy[3], the Policies on Intellectual Property for staff and students[4], the Data Protection Policy[5] and the University of Lancashire's Ethical Principles for Teaching, Research, Consultancy, Knowledge Transfer and Related Activities[6].

Externally-funded researchers must ensure compliance with their funder's policy on research data management and data publication. In cases where researchers may be affected by a number of policies, funder policy should take precedence.

Additional guidance, templates and training materials on research data management are available through the Open Research Team's RDM intranet pages[7].

Researchers working with human participants or sensitive data should also consult the

[2] Formerly UCLanData
[3] Open Access Policy 2023
[4] University of Lancashire IP Policy
[5] Data Protection Policy
[6] Ethical Principles for Teaching, Research, Consultancy, Knowledge Exchange and Related Activities
[7] Research Data Management

University's Human Participant Research Data Management Policy Statement[8] for detailed guidance on consent, de-identification, and secure storage.

5. Data Management Planning

All researchers should develop a Data Management Plan (DMP) at the outset of their research project, regardless of whether it is funded or unfunded. The DMP should form the basis of data management throughout the various stages of the research lifecycle. The Grants and Funding Unit (GFU) will advise whether a research funder requires a DMP to be included in the grant application.

Researchers and PGRs should use DMPOnline, the University's preferred platform for creating and maintaining DMPs. Templates and funder specific guidance are available within the system to support consistency and compliance.

DMPs should address the creation, management, storage and sharing of research data as well as the production of descriptive metadata to aid discovery and re-use.

Where a DMP is a requirement of funding or grant application/s, researchers must work with the Research Data Management Officer and GFU to ensure good practice in research data management and the development of DMPs to a consistently high standard.

Research data must be stored appropriately and securely throughout the life of the research project in accordance with guidance from LIS and relevant institutional policies including the IT Security Policy.

Researchers likely to generate very large datasets exceeding storage provided as standard by the institution[9] must work with the Research Data Management Officer and Learning and Information Services (LIS) to identify a suitable storage solution.

Researchers should ensure that the costs of research data management and any additional data storage required are included in grant applications to external funders, where permitted.

Unfunded researchers must be able to cover the cost of any additional data requirements (beyond standard availability) through School, Institute or central budgets, and this must be agreed before commencement of research.

6. Roles and Responsibilities

6.1 The University

The University is responsible for the provision of a managed repository service for the secure archiving, preservation and long-term storage of completed digital research data and open-access research publications, including journal articles and conference papers. It provides training, guidance and infrastructure through the Research & Knowledge Exchange Service to

[8] Human Participant Research Data Management Policy Statement

[9] LIS provide guidance on standard institutional data storage limits and researchers are expected to access this guidance in order to ascertain whether their data will breach institutional limits.

support good research data management, including the use of DMPOnline and the deposit of research data in Lancashire Online Research Data.

6.2 Researchers

Overall responsibility for research data management during any research project lies with the most senior University of Lancashire researcher (the Data Steward for the project). In cases where the project is led by an external partner there is still a requirement for data generated or shared by the University of Lancashire to be managed by a named individual at the University of Lancashire.

The Data Steward of any externally-funded project should meet with the Research Data Management Officer at regular intervals during the project lifetime, to be agreed at the post-award meeting.

Lead University of Lancashire authors of published research are responsible for ensuring compliance with funder and University policy regarding open access to research papers and the underlying data. Published papers must acknowledge funders, where applicable, and include a short Data Access Statement (DAS)[10] describing how and on what terms any supporting research datasets may be accessed.

6.2.1 Doctoral Supervisors

Where a researcher supervises doctoral students, they should be aware of their responsibilities for ensuring the storage, retention and appropriate management of PGR datasets. Supervisors should follow the Graduate Research School guiding principles for Research Supervisors,[11] specifically;

- To assist PGRs with identifying any IP rights arising in or from their work and keepingthis under regular review throughout the programme of study;
- To ensure that PGRs understand how their research data are stored, managed and where applicable, securely deleted in accordance with University policies;
- To ensure the appropriate storage, archiving or deletion of PGR student data following completion of studies;
- To ensure that upon completion of studies PGRs remove and dispose of all data,equipment, materials and personal belongings appropriately and in a timely fashion;
- To advise PGRs of the requirement to ensure that their thesis and any relevant supporting data are deposited in the institutional repository;
- To support PGRs in developing and maintaining a data management plan using DMPOnline and in preparing datasets for deposit in Lancashire Online Research Data or another appropriate disciplinary repository.

[10] For advice on writing a clear and compliant Data Access Statement, researchers should contact the Research Data Management Officer.

[11] The guiding principles for Research Supervisors'

6.2.2 Postgraduate Research Students

PGRs are responsible for managing the research data generated during their studies under the guidance of their Director of Studies/Supervisory Team. They are required to create and maintain a data management plan in DMPOnline, and understand how their data are stored, managed and, where applicable securely deleted in line with University policy. Students are encouraged to deposit datasets and documentation that support their thesis in Lancashire Online Research Data in line with ethical and funder requirements.

6.3 Intellectual Property Rights

Ownership of intellectual property (IP) created by University of Lancashire staff is outlined in the University Policy on Intellectual Property (Section 3). IP which has potential exploitation (commercial and non-commercial) or publicity value or could otherwise enhance the reputation of the University of Lancashire should be identified and disclosed to the University at the earliest opportunity. The associated data may need to be withheld for a limited period of time (see point 6) to protect IP that would otherwise be compromised.

6.4 External Collaborations and Contracts

Where a project involves external collaborators, the lead organisation is responsible for putting appropriate formal agreements in place covering the contributions and rights of the various organisations and individuals involved. All such agreements should be reviewed andapproved by the University before the project begins.

Except where this is a condition of funding, exclusive rights to research data must not be handed, sold or licensed to external parties.

7. Data Sharing and Preservation

All researchers should familiarise themselves with and comply with the UK GDPR and the Data Protection Act 2018 to ensure any sharing of research data complies with applicable legislation. Data protection guidance for researchers is available to staff on the intranet and can be shared with PGRs by supervisors. Data that has been selected for retention should not be deposited with any organisation that does not commit to its access and availability for reuse unless this is a condition of fundingor would prevent commercial interests.

All digital research data that has been selected by the Data Steward or research group for retention should be deposited in the University of Lancashire data repository or a suitable national or international data service or subject repository within 12 months of generation. As a minimum, where a dataset underpins published research, every effort must be made to ensure its availability on open access at the **date of publication** or before.

All datasets should include comprehensive metadata and a Data Access Statement describing how and on what terms data can be accessed or why it is restricted. Data should adhere to the FAIR principles (Findable, Accessible, Interoperable, and Reusable).

Research data that has been selected for retention should be registered with the University of

Lancashire's data repository, even where the data has been deposited in an external repository or if the data is not suitable for open access. Datasets can be registered by creating a metadata-only record which must contain a stable link, preferably a digital object identifier (DOI) to the externally-held data, where applicable.

Funders typically regard non-deposit of research data as an exception, therefore researchers should make every effort throughout the project to ensure data can be shared openly. Legitimate reasons for non-deposit of data include ethical, legal and commercial constraints; where feasible, issues preventing data sharing should be identified prior to data generation.

The funder should always be made aware of any constraints on access and researchers must be prepared to provide evidence justifying non-deposit. Where the risk has a limited time span, researchers should ensure a publication plan is in place. Data that is withheld or temporarily embargoed should still be managed and held in a format that would permit sharing in event of, for example, a Freedom of Information request or random audit by a funder.

If the research data are to be deleted or destroyed, for example because its agreed period of retention has expired or due to ethical or legal reasons, this should be done so in accordance with all legal, ethical, research funder and collaborator requirements, and with particular concern for confidentiality and security. Any action taken should be documented and retrievable, for possible future audit.

8. Sensitive Data

For the purposes of this policy, sensitive data refers to research data that requires additional controls due to legal, ethical, contractual, security, or commercial considerations. Sensitive data may include personal data, including special category personal data, as well as non-personal data, such as commercially confidential or security-sensitive information.

The University's Ethical Principles for Teaching, Research, Consultancy, Knowledge Transfer and Related Activities provides guidance on approaches to handling sensitive data.

Where research involves the collection or processing of personal data, including sensitive personal data, researchers must ensure that data protection and privacy requirements are considered at all stages of the project, in line with the University's Data protection guidance for researchers and the Human Participant Research Data Management Policy Statement.

Where sensitive data does not constitute personal data, researchers must ensure that appropriate safeguards are in place in accordance with relevant ethical, contractual, commercial, or security requirements.

8.1 Security-sensitive Data

Security-sensitive research material relates to any data - digital or analogue - that can be

interpreted as contravening counter-terrorism legislation under the Terrorism Act (2006)[12]. This Act outlaws the dissemination of records, statements and other documents that can be interpreted as promoting or endorsing terrorist acts or extremism; making explosives/radioactive devices that have a military (or hazardous) purpose and trespass on nuclear sites; and IT encryption design that could pose as a threat to national security.

Any such data must be stored and managed off the University network and according to guidelines set out in the Universities UK document 'Oversight of security-sensitive research material in UK universities[13]. Researchers and research students working with or generating security-sensitive data must liaise with the Research Data Management Officer to ensure compliance with Government regulations.

9. Policy Review

The Open Research Steering Group (ORSG) will be responsible for reviewing and recommending updates to this policy to the University Research, Knowledge Exchange and Ethics Committee every three years, or sooner if required by changes to legislation, funder policy, or institutional systems.

Associated policies, including the Human Participant Research Data Management Policy Statement, will be reviewed on the same cycle to ensure alignment and consistency.

Next Review Date: January 2029

[12] http://www.legislation.gov.uk/ukpga/2006/11

[13] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2012/oversight-of-security-sensitive-research-material.pdf