University of Central Lancashire

Research Data Management Policy

Document type	Policy
Document owner	Research Services
Approved by	Open Research Steering Group – 28 January 2020 University Research and Innovation Committee - 26 February 2020 Academic Board – 18 March 2020
Review date	January 2021
Version	3.0
	Amended July 2019; September 2019
Summary of changes	- Inclusion of information on how researchers can fulfil their data management obligations - References added to the Concordat on Open Research Data and various other procedures since the last version.

Research Data Management Policy

1. Introduction and purpose

In reference to institutional research policies it is useful to define what constitutes research. UCLan defines research in line with the Frascati Manual definition of research and experimental development[1] and in accordance with the REF2021 definition; "research is defined as a process of investigation leading to new insights, effectively shared"

As an institution, UCLan 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 UCLan'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 UCLan and aims to contribute to readiness for future Research Excellence Framework exercise or similar requirements.

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 Common Principles on Data Policy, the Wellcome Trust Policy on Data Management and Sharing, Horizon 2020 Guidelines on Open Access to Scientific Publications and Data 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 UCLan 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

- Contribute towards a culture of openness and transparency

- Establish data deposit as an integral part of the open access process

---

[1] https://www.ref.ac.uk/media/1092/ref-2019_01-guidance-on-submissions.pdf, p.90;
https://www.oecd.org/sti/frascati-manual-2015-9789264239012-en.htm, p. 44

- 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

- All academics at UCLan who produce or work with data generated as a result of research, regardless of how that research is funded;

- All academics who supervise or co-supervise postgraduate research students;

- All postgraduate research students.

4. Policy Awareness

All researchers should familiarise themselves with relevant UCLan policies, in particular this Research Data Management Policy, the Open Access Policy[2], the Policies on Intellectual Property for staff and students[3], the Data Protection Policy[4] and UCLan's Ethical Principles for Teaching, Research, Consultancy, Knowledge Transfer and Related Activities[5].

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.

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 not funded. The DMP should form the basis of data management throughout the various stages of the research lifecycle. Grants and Funding Unit (GFU) will advise whether a research funder requires a DMP to be included in the grant application.

---

[2] https://intranet.uclan.ac.uk/ou/rio/openaccess/SitePages/Home.aspx
[3] https://intranet.uclan.ac.uk/ou/innovation-and-enterprise/
[4] https://www.uclan.ac.uk/data_protection/assets/data-protection-policy.pdf
[5] https://www.uclan.ac.uk/students/research/files/Research_ethical_principles_Oct2012.pdf

DMPs should address the creation, management, storage and sharing of research data and the production of descriptive metadata to aid discovery and re-use. Researchers should use the UCLan, funder or generic DPM templates available in the Digital Curation Centre's DMPonline[6].

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 they are following good practice in research data management and to develop DMPs of 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. See; IT Security policy and Sharing documents and Data policy Researchers likely to generate very large datasets exceeding storage provided as standard by the institution[7] must work with the Research Data Management Officer and Learning and Information Services (LIS) to identify a satisfactory 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 excessive data requirements (beyond standard availability) through Faculty or School 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 secure archiving, preservation and long-term storage of completed digital research data and open access research publications, including journal articles and conference papers. The University provides training, support and advice on all aspects of research data management.

6.2 Researchers

Overall responsibility for research data management during any research project lies with the most senior UCLan 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 UCLan to be managed by a named individual at UCLan.

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 UCLan 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 statement describing how and on what terms any supporting research datasets may be accessed.

---

[6] https://dmponline.dcc.ac.uk/

[7] 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.

6.2.1 Doctoral Supervisors

Where a researcher supervises doctoral students he/she should be aware of supervisor responsibilities with regard to ensuring retention of key PGR datasets. They should follow the guidelines within the UCLan Code of Practice Relating to the Supervision, Examination and Administration of Research Degrees and the Graduate School guiding principles for Research Supervisors,[8] specifically;

•   To assist PGRs with identifying any IP rights arising in or from their work and keeping this under regular review throughout the programme of study;

•   To ensure the appropriate storage 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 arrange appropriate storage and/or archiving of PGR student data upon completion of studies;

•   To advise PGRs of the requirement to ensure their thesis, plus relevant data is deposited into the institutional repository

6.2.2 Postgraduate Research Students

Primary responsibility for the management of data produced during research activities lies with the student, overseen by the Director of Studies/Supervisory Team

6.3 Intellectual Property Rights

Ownership of intellectual property (IP) created by UCLan 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 UCLan 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 and approved 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.

---

[8] These principles are currently in draft but it is anticipated that they will be ratified

7. Data Sharing and Preservation

All researchers should familiarise themselves with and comply with GDPR and DPA regulations on data sharing.

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 funding or 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 UCLan 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.

Research data that has been selected for retention should be registered with UCLan'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

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 of personal data, researchers should work within the guidelines set out in UCLan's [Data Protection Policy](#)

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)[9]. This Act outlaws the

---

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

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'[10]. 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 University Research and Innovation Committee will be responsible for approving this policy as recommended by the Open Research Steering Group. The policy will be reviewed at least annually by the Open Research Steering Group and updated as deemed necessary.

Next Review date January 2021

---

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