University of Liverpool

Policy on Research Data Management

Document Number	RDM-PLN-POL_006
Title	**Policy on Research Data Management**
Version Number	04
Document status	Active
Effective Date	02 December 2013
Review Date	28 February 2017
Author	Alison Fairclough
Approved By	Research and Knowledge Exchange Committee 2 December 2013
Implemented by	RDM Project Manager
Monitoring of compliance	Research Data Manager
Comments	This document was updated in line with an RDM Steering Group review in February 2016

Policy on Research Data Management
March 2015

1. Introduction

University research is conducted in an increasingly complex and data-oriented environment which requires the effective collection, management and sharing of data. The University of Liverpool (UoL) recognises that accurate and accessible data created during the research process are fundamental to the conduct of high quality research and promotion of research integrity. Data are a key asset that will continue to yield benefit for the creator, institution and the wider public well beyond the life of the project.

As part of the University's commitment to academic excellence, this policy seeks to outline key principles for effective curation throughout the lifecycle of data. This policy, and its implementation, will be kept under regular review by the Research and Knowledge Exchange Committee.

2. Scope

This policy applies to all members of the University conducting research or involved in the creation, collection or curation of research data. This policy encompasses all research data that have the potential for publication, regardless of whether or not the research is funded. Where research is supported by a contract or grant that contains conditions on the treatment and ownership of research data, the conditions of this contract or grant is expected to take precedence.

Research data are defined as any recorded information necessary to support or validate a research project's observations, findings or outputs, regardless of format. It includes research in all disciplines but it is recognised that current practices, knowledge and experience varies across and within Faculties, in line with discipline norms. During implementation, Faculties will ensure that all processes and support materials are tailored to different disciplines, reflecting varying research processes, data formats and the potential or opportunity for re-use. For administrative records arising from research projects (i.e. research grant documentation, consent forms etc), please refer to the University's policy on Records Management.

3. Data Management Principles

3.1 Ownership

Primary responsibility for the management of data produced during research activities lies with the Principal Investigator. Where research is conducted with other institutions and independent researchers, Liverpool researchers are responsible for the management of research data held by UoL that is under their own control. In cases where UoL is not leading collaborative research, the PI representing UoL should bear responsibility for familiarising themselves with the UoL policy and ensuring that the discovery metadata of the research is recorded within the UoL metadata catalogue, even if the data themselves are held elsewhere. All research data generated by UoL academics are wholly owned by the University (or funder) and remain with the University if the academic leaves the institution.

3.2 Data management plans

Funders increasingly require grant holders to produce Data Management Plans (DMPs), sometimes also referred to as Technical Plans, at the bid preparation stage. These plans should be kept up to date after funding is granted and as the project progresses. This is good practice that should be followed for all new research projects.

DMPs typically include information describing what kind of data will be created, how it will be stored, organised, shared and archived, keeping in mind any ethical issues that may apply to the information. Guidance and training will be provided by the University. Research data should be classified in accordance with the Information Asset Classification Policy. This classification is likely to vary at different stages of the research project, and this should be reflected within the research data management plan.

3.3 Storage

Across disciplines at the University, research data should be:

- Stored with appropriate metadata to facilitate reuse;

- Secure, safe and backed up regularly (where local storage is chosen, this should be on University networked drives);

- Stored in a manner that is compliant with legal obligations and the requirements of funding bodies and project-specific guidelines;

- Stored in a compliance with other University policies such as Information Asset Classification and Information Security Policy.

The storage and management of research data carries a cost, particularly if there is a need for long-term curation, requiring staff and equipment resources. These costs should be written into research grant applications, where possible. Early planning of data management can significantly reduce costs. Computing Services should be contacted before procuring any data storage equipment for advice on the best storage options.

If equipment is either purchased or procured for the purpose of managing or storing research data the IT Procurement Policy should be consulted. If said equipment is disposed of this should be done in line with the IT Asset Disposal Policy.

Users are liable and responsible for the security of data whilst working off site and detailed guidance is provided in the Code of Practice for use of Data on Laptops and Mobile Devices. If cloud storage is being considered the Code of Practice for Using Cloud Services draws attention to security concerns of data managed through cloud based software.

3.4 Retention
Data, (as defined in the scope of the policy as any recorded information necessary to support or validate a research project's observations, findings or outputs, regardless of format) must be retained in an appropriate format and storage facility for the period of time specified by the funder as a minimum or, in the absence of any funder requirement, a period of at least 10 years. If research data are to be deleted or destroyed, this should be done so in accordance with all legal, ethical, and research funder requirements and with particular concern for confidentiality and security. Records Management have a retention schedule to assist University staff although Research Data is acknowledged as a complex issue within this document and researchers are encouraged to make an assessment using institutional guidance whilst bearing in mind specific funder requirements. Any deletion of data must also comply with the Information Security Policy and the Records Management Office can assist with any confidential waste destruction.

The Data Protection Policy also provides guidance for both storage and data retention. The guidance notes accompanying the policy outline the main points that specifically relate to personal data used for research purposes.

3.5 Access and sharing
All research data produced by UoL researchers should be made openly available with as few restrictions as possible in a timely manner. Except where:

- The rights of individual researchers, or the subjects would be compromised.

- The research has an Intellectual Property opportunity arising from it, in alignment with the Intellectual Property Policy.

- It includes secondary data that you may have had the right to use, but do not have the right to share with others.

Discovery metadata from all research undertaken by University of Liverpool researchers, irrespective of where the data is stored, or whether the University plays a collaborative or lead role, should be recorded within the Universitys metadata catalogue. This metadata catalogue should allow others to understand what research data exists, why, when and how it was generated, how to access it and any access restrictions.

The route you take to making your data open will vary according to your research discipline and environment. Published results should include, if applicable, a statement on how to access the supporting data. This will often depend on the funder stipulations i.e. all published EPSRC funded research must include such a statement, including details on access restrictions and a simple direction to interested parties to 'contact the author' would not normally be considered sufficient. Data should be anonymised prior to disclosing, sharing or publishing in line with guidelines within the Information Asset Policy and adhering to the Data Protection Policy.

Freedom of Information requests that relate to research data should be directed to the Legal, Risk and Compliance department.

Positive initiatives for sharing research data will be recognised through the University's award and recognition processes (Annual Review, Staff rewards etc.).

4. Relationships with other University policies

REGULATIONS, POLICIES AND CODES OF PRACTICE

The regulations and policies apply to all members of staff, visitors, honorary members and all students of the University. The Codes of Practice help all members in adopting best practice
http://www.liv.ac.uk/csd/regulations/.

CODE OF PRACTICE FOR USING THE DATA NETWORK

The Use of the University Data Network is subject to the JANET Acceptable Use Policy:
http://www.ja.net/company/policies/aup.html

CODE OF PRACTICE FOR USING THE CLOUD SERVICES

http://www.liv.ac.uk/media/livacuk/computingservices/regulations/codecloud.pdf

DATA SHARING AND FREEDOM OF INFORMATION

http://www.liv.ac.uk/freedom-of-information/

POLICY ON EXPLOITATION AND COMMERCIALISATION OF INTELLECTUAL PROPERTY

http://www.liv.ac.uk/media/livacuk/hr-migrated/policies/Intellectual-Property-Policy.pdf

ASSET CLASSIFICATION POLICY

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another. The Information Asset Classification Policy and its associated policies are concerned with managing the information assets owned by the University and used by members of the University in their official capacities.

http://www.liv.ac.uk/media/livacuk/computingservices/regulations/information-asset-classification-policy.pdf

INFORMATION ASSET DISPOSAL POLICY

http://www.liv.ac.uk/media/livacuk/computingservices/regulations/it-asset-disposal-policy.pdf

IT PROCUREMENT AND THIRD PARTY SECURITY

http://www.liv.ac.uk/media/livacuk/computingservices/regulations/IT-procurement-policy.pdf

INFORMATION STRATEGY

Our Strategic Plan 2009 – 2014 recognises the importance of Information in achieving our key ambitions.

http://www.liv.ac.uk/csd/regulations/strategy

INFORMATION SECURITY POLICY

This Information Security policy can be summarised as the preservation of confidentiality, integrity and availability which is informed by the principles set out in IS0 27001.
All members of the University are directly responsible and liable for the information they handle. Failure to comply with this policy, and other associated policies, may result in disciplinary action.

http://www.liv.ac.uk/media/livacuk/computingservices/regulations/informationsecuritypolicy.pdf

DATA PROTECTION POLICY

The University must comply with the Data Protection Principles which are set out in the Data Protection Act, 1998.

http://www.liv.ac.uk/legal/data_protection/policy/

And accompanying guidance notes may be found below:

https://www.liv.ac.uk/legal/data_protection/guidance_notes/

RESEARCH ETHICS

A member of the UK Office for Research Integrity (UKRIO), the University is committed to supporting the University's strategic objective of research excellence through its application of robust policies around Research Integrity and Ethics. Any equipment bought for the purpose of research should be purchased in accordance with the Research Related Equipment Policy.

http://www.liv.ac.uk/research-integrity/

RECORDS MANAGEMENT POLICY

The administrative records form a research project will be under the remit of the Records Management Policy. This policy applies to all records created, received or maintained by staff in the course of carrying out their duties, or by researchers engaged on internally or externally funded projects rather than the data itself. The records may be in any format or medium, including electronic media. **Please note that all members of University staff are subject to this policy.**

http://www.liv.ac.uk/library/records-management/policy.html

http://www.liv.ac.uk/library/records-management/services/records_management_policy.pdf

Other departments referenced within this policy:

Records Management

http://www.liv.ac.uk/library/records-management/

Computing Services Department who can be contacted at helpdesk@liverpool.ac.uk

https://www.liv.ac.uk/csd/

Legal, Risk and Compliance

https://www.liv.ac.uk/legal/