

RESEARCH DATA MANAGEMENT AND OPEN DATA POLICY

Background

1. The University of Bristol recognises research data¹ as a valuable institutional asset to be managed in line with UKRI Common Principles on Data Policy². Good research data management enables research data to be securely stored, shared where appropriate, allows the verification of findings and supports digital preservation. In addition, the University acknowledges the role that good research data management can play in underpinning and realising its vision to be recognised globally for the quality of its research.

2. The purpose of this Policy is to provide guidance and support on the responsibilities of the University and its staff in managing and preserving current or future research data. Consideration will also be given to legacy outputs that have value to the University.

Ownership of Data

3. In general the following principles apply:

- Where research is carried out under a grant or contract, the terms of the agreement will determine ownership and rights to exploit the data;
- Where no external contract exists, the University normally has ownership of primary data generated in the course of research undertaken by researchers in its employment;
- The University does not automatically own student Intellectual Property (IP), although in some circumstances students may be required to assign IP to the University. For example, where research is carried out under third-party contract or funding or where the data is produced under third party contract or funding and /or with the significant involvement of University employees.

Policy Scope and Definitions

4. This policy applies to all research conducted by University staff and postgraduate research students (PGRs) regardless of whether or not the research is externally funded. The policy does not currently apply to taught postgraduate students or undergraduates (apart from in exceptional circumstances).

5. Research data is defined as “Data, or units of information which are created in the course of funded or unfunded research, and often arranged or formatted in such a way as to make them suitable for communication, interpretation, and processing.” Examples of research data may include a spreadsheet of statistics, a sound recording of an interview, a descriptive record of a rock specimen or a collection of digital images.

6. A Data Steward is an employee of the University of Bristol who has responsibility for ensuring the proper administration, oversight and security of a dataset generated in the course of their research. The Data Steward may often also be the Principal Investigator (PI) for the research but in some projects data management responsibility may be passed on to another member of the team. If the Data Steward leaves the University they must ensure that they have passed on stewardship for the research data before they leave the organisation (this might involve moving the ownership and responsibility to another institution). Please see paragraph 18 for more information.

¹ For definition of this and other terms please visit <http://www.dcc.ac.uk/digital-curation/glossary>

² UKRI Common Principles on Data Policy, <https://www.ukri.org/funding/information-for-award-holders/data-policy/common-principles-on-data-policy/>

Researcher Responsibilities

7. The Principal Investigator (PI)/ Data Steward of a project has ultimate responsibility for research data management and should ensure that a Data Management Plan is written before the research commences. Data Management Plan guidance for specific funders is available from the University's Research Data Service website³. In practice the day-to-day management of research data may be shared with other researchers involved in a project.
8. Researchers should take into account any likely costs for storing and managing their research data during the lifetime of the project. The time and cost for storage and management should be explicitly written into research applications, including instances where data will need to be made publicly available or curated for many years beyond the project lifetime.
9. Researchers should ensure that research data is stored with appropriate security.
10. Researchers must ensure that they abide by licences or terms of use when using or sharing third party data.
11. The interests of the research participants must be considered at all times, in line with the University's information security policies⁴ and Ethics of Research Policy and Procedure⁵.
12. Researchers are encouraged to publish data in an appropriate digital format (i.e. non-proprietary) wherever possible, in order to facilitate data re-use.
13. Researchers should record significant primary research datasets through the University's research information system (Pure).
14. Upon completion of a significant phase of research activity, research data that a Data Steward feels underpins a published research output or will be of wider use to the research community should be deposited in the University's Research Data Repository (or other repository) in a form suitable for long-term retention and, where possible, wider publication.
15. Researchers should ensure that published research outputs include a statement on how to access any supporting data.
16. Except where this is a condition of a grant or contract, exclusive rights to research data must not assigned, licenced or otherwise transferred to external parties.
17. Where research is conducted in collaboration with external research partners, the researcher should work with the Contracts team in RED⁶ to ensure that suitable agreements for the ownership and use of research data are established and agreed in writing by the parties concerned before the project starts.
18. If the PI leaves the University either during the course of the Research or after its completion, they must pass on the stewardship of any research data created during their employment before their departure, which may include transfer to their next institution where agreed by all parties. In the absence of an agreed successor for the data the stewardship will devolve upwards to the Heads of School or Faculty Dean.

³ <http://www.bristol.ac.uk/staff/researchers/data/writing-a-data-management-plan/>

⁴ <http://www.bristol.ac.uk/infosec/policies/>

⁵ http://www.bristol.ac.uk/media-library/sites/red/documents/research-governance/Ethics_Policy_v8_03-07-19.pdf

⁶ <http://www.bristol.ac.uk/red/contracts/>

Postgraduate Research Student and Supervisor Responsibilities

19. It is the responsibility of postgraduate research (PGR) students and their supervisors to ensure that data management is planned and documented at the outset of the research project. A generic Data Management Planning template for PGR students is available to help guide this process.

20. It is the responsibility of both the student and their supervisor to ensure that any third party funded research data is passed on to their supervisor before the student leaves the University.

The University's Responsibilities

21. The University provides a secure Research Data Storage Facility that researchers are strongly encouraged to use. A limited amount of free storage is available to Data Stewards, although a charge may be incurred for larger deposits.

22. The University will preserve and provide access to research data, beyond the duration of a research activity and in accordance with specific retention requirements.

23. The University provides a research data repository to allow researchers to openly publish their data.

24. The University Research Data Repository also provides methods and procedures for controlled access to restricted data for approved external researchers.

25. The University provides advice and support to researchers involved with data management planning.

26. The University offers training and guidance to researchers actively involved with the creation and management of research data.

27. The University offers support to researchers in the process of depositing research data in the University's Research Data Repository or appropriate external data service.

Relationship with Existing Policies

28. This policy should be read in conjunction with the University's other policies and guidelines, such as:

- [Research Governance and Integrity Policy](#)
- [University Ethics Policy and Procedure](#)
- [Data Protection Guidance](#)
- [Freedom of Information Guidance](#)
- [Information Security Policy](#)
- [Open Access to Research Publications](#)
- [Policy for the use of the Research Data Facility](#)
- [Intellectual Property Policy for Students](#)

Approved by: Senate, at its meeting on 19th October 2015.