University of Brighton Research Data Management Policy

1 Introduction and Purpose

The University of Brighton recognises the ongoing value of the data generated as a consequence of research and its benefits to the public or wider academic community. We therefore aim to allow open access to research data wherever appropriate, while recognising that access to some research data may need to be restricted, for ethical or commercial reasons.

This policy defines expectations of Research Data Management (RDM) practice for all research at the University of Brighton. It identifies responsibilities to ensure that research data will be stored, retained, made accessible and disposed of securely in accordance with all legal, statutory, ethical, contractual and funding requirements. This policy applies to any research data created in research projects involving staff and/or research students of the University or data generated by research conducted on University premises or using University resources.

Research Data may be digital or analogue (e.g. paper-based) data that are collected or generated during the course of or as a result of undertaking research. Research data will be created, amongst other routes, through conducting field or laboratory experiments, conducting trials, surveys, interviews, focus groups, practice-based research or analysis of data.

A Principal Investigator is the University employee tasked with delivering a programme of research on behalf of the institution.

A Researcher means any individual undertaking research or involved in the collection, generation or analysis of research data including employees and research students.

2 Ownership and Intellectual Property Rights

The ownership of research data generated by a researcher will be subject to the University intellectual property principles, unless the terms of research grants or contracts determine otherwise.

3 Managing the Research Data during the research project

The Principal Investigator (PI) will define a research Data Management Plan (DMP), when developing a research project proposal using the guidance provided by the University and the Data Curation Centre (DCC) for this purpose. When a project begins, the PI will ensure that all researchers working on it are aware of the DMP and will monitor its implementation during the research programme. The PI will revise the DMP as necessary to reflect changes identified through the course of the research project or programme.

The PI must ensure that throughout the project, research data that are held digitally should be:

- collected and processed fairly and lawfully as this is a condition of the Data Protection Act 2018 and the General Data Protection Regulations (GDPR);
- held securely, be accurate and only held for as long as necessary;
- processed in-line with the research participants’ rights, under the terms it was collected and be relevant, adequate and not excessive;
- stored securely in a format appropriate for the type of research data in question;
• make use of the University-provided data repository for making final, anonymised datasets publicly available, unless the research proposal or grant awarding regulations states that data should be stored within a specific data repository - such as the ones identified by Natural Environment Research Council - provided that data is held within the European Union;
• limited to access by only those that are authorised as part of the research project;
• encrypted during transmission, for example if stored on a USB stick, laptop, or sent over the internet;
• part of a well-managed backup procedure that involves ensuring on a regular basis that any backed-up data can be restored; and
• documented with adequate metadata and/or other documentation that describes the purpose, structure, retention period and format of the data.

All published outputs resulting from the research should include a reference to where the data can be accessed (see 7 below).

4 Processing of personal data

‘Personal data’ is defined as any information by which a natural living person can be identified directly or indirectly. Personal data should only be collected where it is necessary in order to achieve the aims of the research. Any personal data that are being collected or used for research purposes (including signed consent forms and other personal data that do not form part of the research data) must be processed in accordance with the GDPR, and the University’s Data Protection Policy. All research involving the collection or use of personal data is subject to ethics review via the University’s ethics review framework. Research involving the collection or use of special category data as defined by the GDPR (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; and the processing of genetic data or biometric data for the purpose of uniquely identifying a person; data concerning health or data concerning sex life or sexual orientation) may require additional sign-off by the University’s Data Protection Officer.

All personal data should be collected, stored, transferred and handled securely and precautions should be taken to prevent any unauthorised access to it. Paper based documentation (such as signed consent forms) and audiovisual storage such as audio/video tapes or removable camera cards should be kept in a locked cabinet or desk, and should not be left out on desks or tables or in media devices. All human tissue samples (including blood, urine and saliva) should be stored in accordance with local procedures within Schools established to ensure compliance with the Human Tissue Act (both PABS and SASM have Human Tissue Authority licences).

Researchers are advised to store electronically held personal data on their University OneDrive area or on SharePoint Online sites, which are secure and compliant with GDPR and University IT Regulations. You can find information on OneDrive for students here: https://staff.brighton.ac.uk/is/computing/Pages/OneDrive4students.aspx and OneDrive for staff here: https://staff.brighton.ac.uk/is/computing/Office365/Pages/OneDrive.aspx For collaborative projects, an alternative option is SharePoint Online Sites. SharePoint Online sites offer the same security and tools as OneDrive for Business but include shared document libraries and tools for collaborating and communicating within the group, such as announcements and discussion boards. The University also has a network accessed centrally located large capacity file store (Research Central File Store), which should be used where larger file share capacity with regular
backup is required. To access this facility, researchers should contact the Information Services Service Desk (ServiceDesk@brighton.ac.uk). You can find more detailed information on options for data storage here [https://staff.brighton.ac.uk/is/research/Pages/Storage_for_research_data.aspx](https://staff.brighton.ac.uk/is/research/Pages/Storage_for_research_data.aspx).

Personal data should not be stored on removable devices such as USB sticks, laptops or external hard drives. External cloud based services (such as Survey Monkey, Google docs and Drop Box) should not be used for the collection, storage or transfer of personal data as the servers on which they are hosted are outside the European Economic Area and the GDPR prohibits transfer outside the EU without appropriate safeguards. If you are unsure whether the system you wish to use is recognised and authorised by the University and GDPR compliant, or if you need a product to do a specific task, please contact Information Services Service Desk who can advise you on products that are currently available, or if there is sufficient demand can look to purchase or recommend a product. Where there is a need to transfer data electronically, the data should be anonymised prior to transfer, and files should be encrypted or password protected.

5 Sensitive research data or material

‘Sensitive’ research material is understood as any research material which could be misinterpreted by the authorities as having illegal intent in the context of UK law. ‘Materials’ include online, electronic and hard copy sources. Any research involving the access to or storage of such material is subject to the University’s Policy Statement of registration of research involving sensitive material, and researchers should follow the process outlined in the Policy Statement to register their research.

6 Storage and management of consent forms and other personal non-research data

Signed consent forms and other personal data that do not form part of the research data should normally be kept until the end of the project and then disposed of. However, there may be some instances where it is necessary to keep personal data after the end of a project, for example, if participants have given permission to be contacted for end of study reports, or for follow up of some description directly related to the study, or if they have given permission to be contacted for future studies. Once personal data is no longer required it should be disposed of sensitively and securely. Data held in paper form should be shredded, and researchers should contact Information Services regarding secure disposal of electronic data.

7 Storage and management of the final research data set

On completion of the project, the final anonymised research dataset must be cleaned, ensuring compliance with the University’s Data Protection Policy and deposited in the University data repository along with an updated Data Management Plan. Researchers who deposit research data sets in a national or international repository must only do so if conditions for access have been considered and agreed by the Pro-Vice-Chancellor (Research & Enterprise) or delegate and the funding body requires it.

In all cases and wherever else the underlying dataset is stored, PIs must include an entry in the University’s data repository.

Research data that is deposited digitally should follow University guidelines for:

- secure storage in a durable format appropriate for the type of research data in question;
- metadata and/or other documentation that is adequate to enable discovery.
The University expects that the majority of research data will be digitised, however in instances where analogue research data is unsuitable for digitisation, it should be:

- stored securely;
- labelled, indexed or categorised appropriately;
- described in an entry in the University Data Repository.

All research datasets should be held for a minimum period of 10 years from the later date of either the last access, or of the last publication based wholly or in part on the dataset.

Research Datasets shall be retained for longer where:

- an increased retention period is required to meet the University's statutory obligations, contractual obligations or the guidelines of the body funding the relevant research project;
- the results of the research have resulted in a patent application;
- the results of the research become contentious or subject to challenge during the currently agreed retention period, in which case the dataset should be retained pending review and not destroyed or otherwise disposed of until the matter is fully resolved;
- the research has a public interest or longer-term value.

At the time of a scheduled review, each research dataset should be considered for retention, for disposal/destruction, and for potential relaxation of access limitations. Where the recommendation is other than for disposal/destruction a new review date should be scheduled.

Research data must be destroyed in a safe and secure manner, as outlined in the original DMP and entered as destroyed in the research data record in the University Data Repository, along with the reason for deletion.

Where a PI leaves the University, they should liaise with their line manager to ensure that appropriate arrangements are made for the storage and eventual disposal of any research data currently in their possession. Where another member of the project leaves the University, the PI should ensure that arrangements are made for continuity of access to the data for that member of staff if appropriate.

8 Access

Access to research datasets during the course of a research project should be restricted to the collaborators on the research project in the first instance and only made available to other parties if there are no ethical, commercial or contractual issues and only with the permission of the research collaborators. Access to research datasets deposited in, or accessed through, the University Data Repository may be restricted or embargoed by technical means if it is appropriate to do so. Requests for access to restricted datasets will be considered by legal services.

9 Roles and Responsibilities

Responsibility for the application of this policy on behalf of the Vice Chancellor has been delegated to the Pro-Vice-Chancellor (Research & Enterprise) under the governance of the University Research & Enterprise Committee (UREC). Within this policy, the following specific roles and responsibilities for its implementation are as follows:
Principal Investigators and Research Student Supervisors are responsible for the compliance with this policy including the production and implementation of DMPs, secure data storage / back up during the project and the cleansing and deposit of data on completion.

Heads of School are responsible for the promotion and implementation of this policy and for making arrangements for the management of any data left at the University when a member of their School leaves the institution.

The Department of Research, Enterprise and Social Partnerships and the Doctoral College are responsible for awareness raising of this policy, advice on compliance with funders’ requirements including the production of DMPs, ensuring that research data management is embedded in research ethics processes, the provision of training, briefing materials and templates for PIs and supervisors and monitoring compliance of this policy.

Legal Services is responsible for providing training, guidance and advice on GDPR compliance and data protection.

Information Services is responsible for the management and maintenance of University systems designed to support this policy, for providing guidance on data storage procedures, and for providing specialist support in instances of non-standard storage requirements.

10 References

EPSRC Policy Framework on Research Data
UKRI Common Principles on Data Policy

Digital Curation Centre resources:
  Curation Lifecycle Model
  How to Develop a Data Management and Sharing Plan
  Overview of funders’ data policies
  Funders’ [detailed] Requirements
  Guidance and Examples

University of Brighton policies:
  Policy on Research Integrity
  Research Ethics Policy
  Intellectual Property Policy
  Data Protection Policy
  Freedom of Information Policy
  Open Access Policy
  Policy Statement on registration of research projects involving access to/and or storage of sensitive research material
<table>
<thead>
<tr>
<th><strong>Owner</strong></th>
<th>Research, Enterprise &amp; Social Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version number</strong></td>
<td>6.0</td>
</tr>
<tr>
<td><strong>Revision history</strong>&lt;br&gt;(most recent first)</td>
<td><strong>Version</strong></td>
</tr>
<tr>
<td>6.0</td>
<td>Clarify issues around data storage and roles and responsibilities</td>
</tr>
<tr>
<td><strong>Date approved</strong></td>
<td>May 2019</td>
</tr>
<tr>
<td><strong>Approved by</strong></td>
<td>University Research &amp; Enterprise Committee</td>
</tr>
<tr>
<td><strong>Implementation date</strong></td>
<td>May 2019</td>
</tr>
<tr>
<td><strong>Date of next review</strong></td>
<td>May 2022</td>
</tr>
</tbody>
</table>