Research Data Storage Facility

Terms of Use

January 2021

By signing up to these Terms of Use, you are agreeing to abide by the terms of the University's **Policy for the use of the Research Data Storage Facility**.

You should also be aware of the terms of the University's **Research data management and open data policy** - http://www.bristol.ac.uk/research/environment/governance/research-data-policy/ and the University's **Information Security Policies** - http://www.bristol.ac.uk/infosec/policies/

1. Definitions

Data Controller

a person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons e.g. the University.

Data Protection Legislation

means the **UK Data Protection Legislation** and (for so long as and to the extent that the law of the European Union has legal effect in the UK) the General Data Protection Regulations (EU) 2016/679) and any other directly applicable European Union regulation relation to data protection, where "**UK Data Protection Legislation**" means any data protection legislation in force from time to time in the UK including the Data Protection Act 1998 or 2018 or any successor legislation.

Data Steward

an employee of the University of Bristol who has long-term responsibility for ensuring the proper administration, oversight and security of a dataset generated in the course of their research and deposited with the Research Data Storage Facility. Students and honorary staff members cannot be Data Stewards.

The Data Steward's responsibilities include providing such information as might be reasonably required by the Research Data Storage and Management Executive to make an adequate risk assessment for data storage, and to fulfil the University's legal and ethical obligations.

Where the dataset contains personal data, the Data Steward is responsible for ensuring the data is processed in accordance with the University's obligations as a Data Controller under Data Protection Legislation.

The Data Steward is responsible for ensuring that Data Users comply with the Research Data Storage Facility Terms of Use, including any External Data Users whom the Data Steward authorises. Further information about the responsibilities of the Data Steward is set out in the Policy for the use of the Research Data Storage Facility, which should be read alongside this document.

Data User

someone authorised by the Data Steward to have access to the data assets of the project, who is also a member of staff or a registered student of the University of Bristol.

External Data User

someone collaborating with the Data Steward, but is not a member of staff or a registered student of the University of Bristol, who is authorised by the Data Steward to have access to the data assets of the project.

Research Data Service

The University's Research Data Service offers advice, support and training in all areas of research data management and is responsible for the University's Research Data Repository. The service is responsible for developing policies and processes to facilitate the creation, storage, sharing and long-term preservation of research data in order to meet both the needs of the immediate researchers and the ongoing needs of secondary data users.

2. Data protection

2.1 Where an employee of the University of Bristol is processing personal data in the course of their employment, including for the purposes of research, then the University of Bristol will be the Data Controller. The University of Bristol takes its obligations under Data Protection Legislation very seriously, and it is a condition of employment at the University that staff agree to abide at all times by the provisions of Data Protection Legislation in relation to any processing by them of the personal data of others.

http://www.bristol.ac.uk/hr/terms/generalterms.html#a15

Any work involving processing, storing or recording personal data must meet the requirements of Data Protection Legislation. It is the Data Controller's responsibility to ensure that personal data is collected in accordance with Data Protection Legislation.

http://www.bris.ac.uk/secretary/dataprotection

It is expected that personal data collected in the course of research will be anonymised prior to deposit in the Research Data Storage Facility (the Facility). If a Data Steward wishes to store sensitive personal data without anonymising it, they must provide EITHER:

a) an explanation in the Research Data Storage Facility Application Form.; OR
b) a copy of an appropriate Ethics Committee application (e.g. Department, Faculty or NHS) and documented evidence of the relevant Ethics Committee's approval and any conditions.

Please also refer to the Policy for the use of the Research Data Storage Facility.

3. Freedom of Information

3.1 Under the Freedom of Information Act 2000, third parties may request access to information held by Public Authorities, subject to certain exemptions. Such exemptions are interpreted strictly. Universities are defined as Public Authorities under the Act and research data may thus be requested under FOI legislation. An amendment to Section 22 of the Act in 2014 provides an exemption which should protect the majority of ongoing research where there is an intention or requirement to publish the data at some future date –

http://www.legislation.gov.uk/ukpga/2000/36/section/22

The Data Steward must first consult with the University Secretary's Office, and then inform the Research Data Storage and Management Executive, at the time of application, if they believe an exemption to third party access under the Freedom of Information Act 2000 should apply to the data they wish to store in the Facility. They must provide details to the Secretary's Office of why the exemption applies to the data, and how long the exemption should last. If a FOI request is received, whether the exemption applies will be assessed by the Secretary's Office on receipt of the request.

4. Legal and Ethical Reservation

4.1 The University reserves the right to remove data from its computer systems, including the Research Data Storage Facility, without notice to the Data Steward, if that data breaches UK laws, is in breach of ethical standards to which the University and its staff have committed, or otherwise breaches published University policies.

5. Technical issues

5.1 The University cannot guarantee that it will be able to fund the mirroring of large data sets. The final decision will rest with the Research Data Storage Policy owner. Where such storage requirements are known at the outset of the project design, it should be discussed with the Research Data Storage and Management Executive to ensure that it can be accommodated, and any additional costs associated with this can be addressed.

5.2 The Data Steward retains responsibility for the validity of the data.

5.3 The Data Steward retains responsibility for the readability and accessibility of the data.

5.4 For certain data, there may be a requirement to delete the data as after a period of time. Such a requirement must be detailed in the exit strategy in the Data Management Plan or detailed on the RDSF project application form and this requirement should be discussed with the ACRC when the RDSF project is requested. It is the responsibility of the Data Steward to inform the ACRC if any data may need to be deleted, and it is the responsibility of the Data Steward to ensure that data that will need to be deleted is encrypted.

5.5 If data is to be stored offsite, the ACRC will inform the Data Steward. It is the Data Steward's responsibility to confirm whether it is allowable for the data in their RDSF project to be stored offsite. It is also the Data Steward's responsibility to determine whether a Privacy Impact Assessment needs to be completed in relation to offsite storage of their data.

6 Ownership of data

6.1 It is the usual practice for the University to own any intellectual property (IP) arising from research undertaken by University staff unless otherwise agreed with a funding body, subject to a sharing agreement with staff.

6.2 If a member of staff leaves the University, the data should be retained in the Facility as the data belongs to the University. If a Data Steward is intending to leave the University of Bristol, they must inform the ACRC and provide the name of an alternative Data Steward for any data they hold in the RDSF before they leave the University. If no alternate Data Steward is nominated, the outgoing Data Steward's line manager or the Head of School, as appropriate, will be contacted by the ACRC and asked to nominate a successor. If no successor is nominated, the line manager or Head of School will assume the responsibilities of Data Steward until an appropriate alternative can be identified. In exceptional circumstances, the Research Data Storage and Management Executive may agree that an existing Data Steward can take over as Data Steward of the departing Data Steward's project(s) as well, even if this increases the total amount allocated to the existing Data Steward above the current 'free' allocation.

6.3 The University may allow a researcher/Data Steward to take data with them, when they leave the University. Any transfer of data from the facility by a Data Steward/researcher must first be agreed in writing by the University.

6.4 In the case of personal data the University of Bristol, as Data Controller, will require the researcher/Data Steward to sign a personal data transfer agreement, guaranteeing that the personal data will only be processed in accordance with Data Protection Legislation, and that the university to whom the personal data is being transferred will indemnify the University of Bristol against any claims for breach of Data Protection Legislation arising out of that transfer. This must be agreed with the University of Bristol's Secretary's Office.

6.5 Any data stored in the facility by a student associated with his/her thesis will be owned by the student. When the student leaves the University, the data may be withdrawn from the facility by the student, in agreement with the Data Steward.

7 Security/access/reuse

7.1 Only authorised personnel are allowed unsupervised access to the machine rooms. Any visitors must be accompanied by an authorised member of staff.

7.2 The ACRC will put appropriate access controls in place to ensure that only authorised users can access data.

7.3 Users should use encryption where access needs to be further controlled, particularly to sensitive data - http://www.bris.ac.uk/infosec/uobdata/encrypt/file/.

7.4 The responsibility for identifying security requirements for the data remains with the Data Steward. The ACRC will endeavour to comply with this and will advise the Data Steward if security requirements cannot be met. The Data Steward must be familiar with the University's information security policies - http://www.bris.ac.uk/infosec/

7.5 Virus scanning of the data which resides in the Facility will remain the responsibility of the Data Steward, in liaison with IT and ACRC staff. The Data Steward will ensure that all data is virus scanned before it is stored on the Research Data Storage Facility and it is the Data Steward's responsibility to take appropriate action in relation to the results of virus scans.

If the Facility is mounted on a network drive, virus scanning should not take place on that drive. Virus scanning should take place on upload and download from that network drive.

7.6 The security levels available to Data Stewards correspond with the University's information security policy - http://www.bris.ac.uk/infosec/uobdata/classifications. A Data Steward can select Public, Open, Confidential, Confidential and Sensitive, or Secret. Anyone wishing to store data classed as Secret in the Facility will need to talk to the ACRC first.

7.7 In administering the RDSF, the ACRC follows the University of Bristol's 'Guidelines for system and network administrators'. Where necessary to ensure the proper operation of the RDSF, systems administrators may examine files. If this may breach any agreements, policies or legislation in relation to a dataset, a Data Steward **must not** store that dataset on the RDSF. More information is available in the Guidelines:

http://www.bristol.ac.uk/media-library/sites/infosec/documents/sysadmin.pdf

8. Uploading data to *data.bris* Research Data Repository

8.1 Users wishing to publish data should make a folder within the 'Data-Bris' folder in their RDSF project, containing the files and folders they wish to publish. The publication system can see the contents of this folder, and will take a copy of this folder as the published dataset. Once published the original folder within Data-Bris is no longer needed and may be removed.

Publications are held in a separate area where users cannot modify them. However metadata updates and modifications can be requested via the Library's Research Data Service.

The default allocation for the data publishing folder is 100GB, but more can be made available upon request up to a limit of 1TB (subject to approval). Beyond this the storage cost is equal to regular project storage.

8.2 Only a Data Steward can validate data publication. Once the data has been prepared for publication, the Data Steward needs to check it and then approve the publication.

9. Data sharing with External Data Users

9.1 Any storage allocation requested for a Collaboration Project is included in the Data Steward's total storage allocation. If the Data Steward wishes to include a Collaboration Project within their free allocation, the Data Steward may need to request a reduction in their Standard Project allocation to stay within the free allocation overall.

9.2 The Data Steward is the owner of all data in a Collaboration Project, as set out in section 1.9 of the Policy for the use of the Research Data Storage Facility.

9.3 An External Data User can register as a member of a Collaboration Project for a maximum of 3 years. The External Data User can then re-register for a further 12 months, in agreement with the Data Steward.

10. Costs

10.1 The current costs of storing data in the RDSF are set out at

http://www.bristol.ac.uk/acrc/research-data-storage-facility/rdsf-costs/.