Research Data Storage Facility

Terms of Use

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

1. Definition

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 Steward	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 and deposited with the Research Data Storage Facility. The Data Steward's responsibilities include providing such information as might be reasonably required by the Research Data Storage and Management Board 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 the Data Protection Act 1998.[1] 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. The responsibilities of the Data Steward are set out in the Policy for the use of the Research Data Storage Facility sections 1.9-1.14.
Data User	someone authorised by the Data Steward to have access to the data assets of the project, who is also an employee or a registered student of the University of Bristol.
External Data User	someone collaborating with the Data Steward, but is not an employee 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.
data.bris	the University's research data service, currently being developed as a service pilot – http://data.bris.ac.uk. The service is 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.

[1] Personal data are data relating to a living individual who can be identified by that information (or from that and other information in the possession of the data user) including any expression of opinion about the individual and any indication of the intentions of the data user/controller in respect of that individual.

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 the Data Protection Act very seriously, and it is a condition of employment at the University that staff agree to abide at all times by the provisions of the Data Protection Act 1998 in relation to any processing by them of the personal data of others.

http://www.bristol.ac.uk/personnel/terms/generalterms.html#Dataprotection

Any work involving processing, storing or recording personal data must meet the requirements of the Data Protection Act 1998. It is the Data Controller's responsibility to ensure that personal data is collected in accordance with the Data Protection Act.
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 personal data without anonymising it, they must provide EITHER:

a) an explanation in the Research Data Storage Facility Application Form. Please also refer to section 5.5 ; 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.

Proposed storage of unanonymised sensitive personal data[2] will additionally require the Data Steward to provide written approval from the University Secretary's Office.

Please also refer to section 2.3 of 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.

A Data Steward who has a confidentiality agreement covering the data and/or believes an exemption to third party access under the Freedom of Information Act 2000 applies to the data they wish to store in the Facility must:

a) prior to application, consult with the University Secretary's Office; and ,

b) at the time of application, inform the Research Data Storage and Management Board.

They must provide details of why the exemption applies to the data, how long the exemption should be expected to last and terms of any confidentiality agreement. If a FOI request is received, whether the exemption applies will be assessed by the University Secretary's Office, on receipt of the request. Please also refer to section 2.4 of the Policy for the use of the Research Data Storage Facility.

[2] Sensitive personal data are personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences.

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. This applies to data deposited in either a Standard Project or in a Collaboration Project.

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 Board to ensure that it can be accommodated and any additional costs associated with this can be addressed.

5.2. Data Stewards must provide a realistic assessment of how much data is required to be stored as mirrored/highly available or resilient or archived as part of the application process. The Research Data Storage and Management Board may require additional information where a Data Steward asks for all their research data to be held as mirrored or mirrored and resilient.

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

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

5.5. It will be normal procedure for data to be deleted from disks by secure erasing. In the case of sensitive data stored on a disk, there may be a requirement to certify the disk as having been destroyed. Such a requirement to destroy disks must be detailed in the exit strategy detailed in the DMP or on the application form (please refer to section 1.15 of the Policy for the use of the Research Data Storage Facility.) If the file system holding sensitive data becomes corrupted, and data cannot be securely erased, assurance will be sought from the hardware vendor that they can securely erase the data.

If data is stored offsite, the ACRC will check with the Data Steward that this is allowable, if the data being stored is classed as Strictly Confidential or Secret. (Please refer to section 8.6.) The ACRC will also discuss with the Data Steward whether there is a need for a Privacy Impact Assessment (PIA) if personal data, which has not been anonymised, is being stored off site.

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. IP is described as the outputs of creative endeavour in literary, artistic, industrial and scientific fields which can be protected under legislation i.e. the research results –

http://www.bris.ac.uk/research/knowtransfer/ip/ipownership.html.

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 researcher acting as a Data Steward leaves, responsibility for the Data Steward's data assets will be transferred to his/her line manager in the first instance. In exceptional circumstances, the Research Data Storage and Management Board 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.

6.2. 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.

6.3. In the case of personal data the University, 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 the Data Protection Act 1998, and that the university to whom the personal data is being transferred will indemnify the University against any claims for breach of the Act arising out of that transfer. This must be agreed with the Secretary's Office.

6.4. 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 secure password controls in place to ensure that only authorised users can access data.

7.3. Encryption will be used where access needs to be further controlled, particularly to sensitive data.

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 policy - 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 zonal IT and ACRC staff. The Data Steward will confirm on the application form that adequate virus scans will be undertaken before the data is stored in the Facility. Standard practice will be for the data to be virus scanned on the local systems.

If the Facility is mounted on a network drive, scanning should not take place on that drive. Scanning however, should take place on upload and download from that network drive. Local zonal IT support staff should be able to advise on this.

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, Strictly Confidential or Secret. Confidential and Strictly Confidential will have a decreasing number of users able to access the data. Anyone wishing to store data classed as Secret in the Facility will need to talk to the ACRC first.

8. Uploading data to *data.bris*

8.1 If a user wishes to upload data to the *data.bris* repository for publication, he/she needs to create a folder within the relevant RDSF project and move the relevant subset of the data into this folder. Once the data is moved into this folder, it is 'read only' and cannot be altered without application to the RDSMB. **Any data held in this folder is therefore part of the Data Steward's project allocation and will be included in the total amount of storage used by**

his/her project. The default allocation for the data publishing folder is 100GB, but more can be made available upon request.

8.2 Only a Data Steward can validate a data upload, so once the data has been prepared for upload, the Data Steward needs to check it and then confirm the upload.

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 the free 5TB allocation, he/she may need to request a reduction in the Standard Project allocation to stay within the 5TB 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 Any External Data User granted access to the RDSF as part of a Collaboration Project, will be granted 'read only' access as the default setting. The Data Steward can choose to make this access 'read-write'.

9.4 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.

Costs of using the Research Data Storage Facility are set out in a separate document, Costs of using the Research Data Storage Facility.