PRIFYSGOL
BANGOR
UNIVERSITY

Policy Title	Research Data Management Policy
Approval Date	November 2014
Approving Body	University Executive
Version	March 2019 V.5 (Revised and updated)
Supersedes	September 2015
Previous review date	February 2018
Next review date	February 2020
Policy Owner	Library & Archives Service
Lead contact	Michelle Walker (Repository and Research Data Manager) Beth Hall (maternity cover October 2019-October 2020)
Authors	Michelle Walker In consultation with the Access to Data Operations Group: Beth Hall, Graham Worley, Saskia Pagella, Adrian Fewings, Lynette Hunter

This policy is part of Bangor University's commitment to research excellence and advocates that Research data will be managed and stored to the highest standards throughout the research data lifecycle.

There is growing widespread acknowledgment that publicly funded research data are a public good, produced in the public interest, which should be made openly available with as few restrictions as possible in a timely and responsible manner that does not harm intellectual property. As such, Bangor University endorses the UKRI Common Principles on Data Policy[1] and the Concordat on Open Research Data[2].

For the purposes of this policy, data refers to any material (digital or physical) which is used to underpin and validate research findings.

The implementation of this policy will be supported at the School/College and Institutional level as appropriate.

1. The Researcher is responsible for:

1.1. Creating a research data management plan at the beginning of every project that explicitly addresses data capture, management, integrity, confidentiality, retention, sharing and publication. This responsibility lies with the Principle Investigator (PI).

1.2. Working with IT Services to identify storage requirements that may exceed that offered by the institution. See Appendix 1 for detailed Storage requirements of the institution.

1.3. Ensuring the safe storage of all Bangor University research data during a research project.

1.4. Ensuring the University is able to recover actual costs incurred in providing research storage from external funders in order to ensure sustainability of storage services and expand them where necessary.

1.5. Providing sufficient metadata (descriptive information) to the University's PURE repository about their research data to ensure others can discover and, if permissible, reuse it. This also applies to data that is stored outside of Bangor University, for example in an international data service or domain repository.

1.6. Ensuring that published results always include information on how to access the supporting data.

1.7. Making relevant data openly available to other researchers in a timely way, with as few restrictions as possible.

1.8. Ensuring that exclusive rights to reuse or publish research data are not handed over to commercial publishers or agents without retaining the rights to make the data openly available for re-use, unless this is a condition of funding.

1.9. Clearly stating who owns the data that is being generated through the research activity. Where this is not clear, researchers will work with IPR specialist in the Research, Innovation and Impact Office, the Library & Archives Service, and College support teams to verify data ownership as early as possible in the research data lifecycle.

1.10. Ensuring that appropriate measures are put in place to handle sensitive data throughout the lifecycle of a research project. Any particular restrictions on access associated with sensitive data should be taken into account. Researchers should pay particular attention to GDPR and ensure they adhere to the University's policies on data protection.

1.11. Ensuring research data will be offered, assessed and appraised for deposit and retention in an appropriate national or international data service or domain repository, or the University's digital repository PURE.

1.12. Ensuring that research data and records are retained for as long as they are of continuing value to the researcher and the wider research community, and as long as specified by research funder, patent law, legislative and other regulatory requirements. The minimum institutional retention period for research data and records is five (5) years after publication or public release of the work of the research, unless required by the funder to retain for longer. For example the EPSRC state

[1] https://www.ukri.org/funding/information-for-award-holders/data-policy/common-principles-on-data-policy/ (Accessed 20/03/2019)

[2] https://www.ukri.org/files/legacy/documents/concordatonopenresearchdata-pdf/ (Accessed 20/03/2019)

minimum of 10 years from the end of any researcher 'privileged access' or, if others have accessed the data, from last date on which access to the data was requested by a third party.

1. **The Institution is responsible for:**

   1.1. Providing in-project access to services and facilities for the storage and backup of research data and records that allow researchers to meet their requirements under this policy and those of the funders of their research.
   1.2. It is envisaged that in-project storage will cease 6 months after the end of a project, unless a valid request is made to IT Services to extend that time limit.
   1.3. Providing the facilities for post-project deposit and retention of research data when not deposited in a national or international data service or domain repository.
   1.4. Providing researchers with access to training, support and advice in research data and records management.
   1.5. Providing a set of chosen metadata guidelines for the deposit of information relating to Research Data deposit.

Relationship with existing policies:

In addition to compliance with funder's policies, compliance must also be maintained with the following Bangor policies.

1. Academic Integrity in Research: Code of Practice
   https://www.bangor.ac.uk/research-innovation-and-impact-office/BU%20Academic%20integrity%20Final%20V1%200.pdf
2. Acceptable Use Regulations: Regulations for the Use of IT Resources
   https://www.bangor.ac.uk/itservices/policies/acceptable-regulations.pdf)
3. Aberystwyth University & Bangor University Common Intellectual Property Policy
   https://www.aber.ac.uk/en/hr/policy-and-procedure/au-and-bu/intellectual-property/
4. Data Protection Act Policy
   https://www.bangor.ac.uk/governance-and-compliance/dataprotection/documents/Data%20Protection%20Policy%20final%20July%202018%20v6.pdf
5. Record and Data Retention Schedule
6. Freedom of Information Act Policy
   https://www.bangor.ac.uk/governance-and-compliance/freedomofinformation/documents/freedom-information-policy.pdf
7. Information Security Policy
   https://www.bangor.ac.uk/governance-and-compliance/policy-register/documents/information-security-policy.pdf
8. Research Ethics Policy
   https://www.bangor.ac.uk/governance-and-compliance/documents/research-ethics-policy-en.pdf
9. Research Strategy
   https://www.bangor.ac.uk/research-support/documents/Enhancing%20Research%20Success%20at%20Bangor%20May%202014.pdf
10. Bangor University is committed to implementing the principles of the Concordat to Support the Career Development of Researchers
    https://www.bangor.ac.uk/humanresources/staffdevelopment/ConcordatforResearchers.php.en
11. Guidelines relating to Academic and Research Staff leaving the employment of the University
    https://www.bangor.ac.uk/research-innovation-and-impact-office/V1.6%20Guidelines%20relating%20to%20Academic%20and%20Research%20Staff%20leaving%20the%20employment%20of%20the%20University.pdf

For further information and key contacts, please visit Bangor University's Research Data Management webpages

Appendix 1 – Research Data Storage Technical Guidelines

1. Safe Storage of Research Data

1.1. All University research data shall be stored on safe and secure storage during a research project.

1.2. A storage system shall be deemed safe and secure if it can deliver, as a minimum, all of the following functions:

1.2.1. Suffer the loss of a single computer disk with no operational downtime;

1.2.2. Ensure that only authorised individuals may access the data;

1.2.3. Other than when housed securely within the University's data centre encrypts the data;

1.2.4. to guard against possible human error provide a means of recovery of files on a daily basis for the previous month and on a monthly basis for up to three months;

1.2.5. In the event of a catastrophic system failure caused either by human, systemic or environmental factors allow for the restoration of the data from an external backup source.

1.3. The University's main storage services are compliant with this policy and it is these services offered from the NAS device that is normally presented as the familiar M and U drives. The NAS shall be the *preferred location* for all research data during a project's lifetime. Microsoft OneDrive/Teams offers up to 1TB at no additional cost to the University. This shall be the preferred location for most research data unless performance requirements (speed of access) exceed the capabilities thereof.

1.4. In the event that a researcher wishes to use a location other than the *preferred location,* the IT Services department of the University shall determine if that storage system is deemed to comply with these requirements.

1.5. When considering *cloud solutions* for storage the University shall only permit the data to be housed outside of the European Union in extreme circumstances where no other option is viable. Under no circumstances shall any personal data be stored outside of the European Union (legal requirement).

1.6. Systems that have already been deemed appropriate are listed in Point 8. IT Services shall permit the use of these services in the event of the *preferred location* being unsuitable for the requirements of the research project.

1.7. Devices including USB memory sticks, NAS devices, external USB hard drivers, tablet computers, smart phones, desktop computers and laptops by themselves are not considered to comply with these requirements.

2. Working Away – Temporary Storage

2.1. It is accepted that due to the nature of some research it may not be immediately possible to ensure that the data is immediately written to a storage device compliant with this policy. This may be due to the nature of the equipment being used or simply that the researcher is away from the University when the data is collected. Researchers shall ensure that they make every effort to meet the objectives of this policy. In particular when collecting data using laptop devices or similar they shall:

2.1.1. Ensure that a backup of the data is taken and stored on a separate device and preferably kept in a separate location.

2.1.2. When a backup device has been utilised seek to ensure that it is transported back to the University by a different means to that of the device containing the primary data e.g. in another vehicle or by another courier.

2.1.3. Where access to the internet is possible and of sufficient speed, researchers shall transfer the data back to University storage systems or other cloud resources. Microsoft OneDrive can achieve this requirement through the secure sync to cloud from the local device. All such transfers shall be over a secure protocol such as OneDrive, SFTP (Secure File Transfer Protocol) or SCP (Secure Copy) to protect the content, details of which are available from IT Services.

2.1.4. At all times when dealing with data give due regard to the University's data security policy and seek advice from IT Services to ensure data is adequately protected and encrypted when dealing with portable storage devices.

3. Recovery of Storage Costs

3.1. The University shall ensure adequate storage space is available to securely store all research data.

3.2. IT Services shall ensure that the amount of space allocated and used by a research project shall be auditable.

3.3. Whilst planning a research project and completing a *Data Management Plan* a researcher shall make an assessment of the amount of data the project is likely to generate or collect. If this storage exceeds five (5) Terabytes, the researcher shall notify IT Services to ensure that sufficient space exists.[3]

3.4. For provision in excess of 1TB, the University shall recover the costs of the storage system through the normal procedure for overhead recovery.

3.5. If the researcher wishes to purchase another storage solution the researcher shall include the full cost in the research budget (to include costs of management and maintenance for the duration of the requirement) and ensure that University purchasing regulations shall be followed. IT Services shall need to approve the purchase of another storage solution.

4. Data Format, Archival and Preservation

4.1. Researchers should consider the format of the data that they collect whilst planning their research project. If they are unable to store the data in an *open* format, they should ensure that they would have continued access to the specialist software needed to read back the collected data at least until the end of the project. The advice of IT Services should be sought where necessary.

4.2. Most funders require *Data Management Plans* from researchers and these usually require consideration of the long-term preservation of the data collected during research. Where a project funder does not require such a plan the researcher for the benefit of the University shall make an A*bbreviated Data Management Plan* so as to define what data will need to be preserved and the method of preservation following the end of the project.

4.3. As a consequence of the *Data Management Plan* or the *Abbreviated Data Management Plan,* the University shall not be required to continue to offer storage at the *preferred location* after the end of the funded part of the project or the end of the analysis of the data whichever is the later. After this time, the data shall be moved to longer-term repositories where there is continued value in the data.

5. Precedence

5.1. Nothing in this policy shall take precedence over the IT Security Policy or the IT Acceptable Use Policy of the University.

6. List of Approved Storage Services

Amazon S3 Glacier
Suitable for archive storage only after data is processed. Not suitable if researcher anticipates frequent reading of data.

Amazon S3 Standard
More suitable for changing data still expensive to read data from. Particularly suited when data is processed and distilled to a smaller output using compute power provided (at extra cost) from the Amazon Cloud.

Microsoft OneDrive
Suitable for most research data needs where the files are small and speed is not a critical factor. Typically, this would be spreadsheet, word processor and similar files. Unsuitable for large data sets that need to be accessed quickly, such as numerical computing output. Currently free as part of Office 365 and gives up to 1Terrabyte of storage.

[3] *1000 Gigabyte = 1 Terabyte, 4.7Gigabyte is the approximate size of a DVD, 0.6 Gigabyte is the approximate size of a CD-ROM. Typically 1 Gigabyte can store around 500 camera images or 100 MP3 music files depending on their quality.*