Coversheet:

Author	Noelle McDougall and Jim Huntingford
Equality Impact Assessed by	Rapid Impact Assessment completed; Comprehensive review not required
Approved by	Senate
Approval date	June 2018
Review date	July 2019
Version	Version 1.1
Document type	Policy
Activity/Task	
Document location	https://intranet.abertay.ac.uk/documents/policies-and-procedures/research/
Linked documents or legislation	Complying with GDPR at Abertay: GDPR Research Policy Document

End of document (details):

Version Number	Purpose / Changes	Author	Date
Version 1.1	New UKRI link added	Noelle McDougall	18/9/2018

Abertay University

Research Data Management Policy

Executive Summary

1. This policy is binding on all University members engaged in research, including staff and PGR students, but does not apply to postgraduate taught and undergraduate students, except where there is a reasonable prospect that their research findings are/will be included in published research outputs.
2. Before a project begins, a research Data Management Plan (DMP) must be completed.
3. Data collected during a project must be stored on the University network, to ensure it is suitably protected against accidental loss or damage and against unauthorised access.
4. Data with acknowledged long-term value must be preserved and also made openly accessible with as few restrictions as possible unless there are compelling reasons not to be so.
5. A metadata record describing retained data must be made publically available via Pure, within 12 months of the data being generated, even if access to the final dataset(s) itself is restricted.
6. Research publications must include a data access statement.
7. In line with UKRI policies, researchers are entitled to a limited period of privileged access to the data they collect to allow them to work on and publish their results.
8. Data that cannot be digitised must also be registered in Pure, stored securely and organised in a manner that would facilitate it being shared in the event of a valid request for access being received.
9. Use of others' data should always conform to legal, ethical and regulatory frameworks including appropriate acknowledgement.
10. Data must always be managed, throughout its lifecycle, in compliance with all relevant legal, ethical, and regulatory frameworks, and in the case of personal information, the provisions of legislation and University policy relating to GDPR.

Research Data Management Policy

Purpose

This policy aims to ensure that our research data management practices meet the highest standards and are aligned with the UKRI Research Council Common Principles on Data Policy[1], and the Concordat on Open Research Data.[2] It sets out the University's expectations so that all stakeholders recognise their responsibilities and obligations and can contribute to data being maintained and preserved as identifiable, discoverable, retrievable and reusable assets.

Scope

This policy is binding on all University members engaged in research, including staff and research students, and those who are conducting research on behalf of the University. The Policy does not apply to postgraduate taught and undergraduate students, except where their research findings are included in published research outputs.

Implementation

An evolutionary approach will be taken to implementing this policy with a target date of 2022 set for full implementation. A research data roadmap will help the University achieve this goal and progress will be reviewed regularly. Initially, priority will be given to ensuring funder requirements are met and/or to research where the results have potential for publication. **For funded projects, the requirements of this policy are mandatory from the date of this policy onwards**.

The University expects all research data with potential long-term value will eventually be managed to the same standards, but recognises that extending the scope of this policy beyond those engaged in funded research will be a longer-term endeavour.

In light of the pace of change in this field, this policy will be reviewed 12-months from the date of approval.

Principles

1. Good data management is fundamental to all stages of the research process and the highest standards must be applied throughout the data lifecycle, from creation to preservation or disposal.

2. Data with acknowledged long-term value should be preserved and be made discoverable and openly available with as few restrictions as possible in a timely and responsible manner.

3. Open access will not be possible in cases where there are justified and justifiable legal, ethical and commercial constraints on data release.

4. Conditions of grant from individual funding bodies with specific guidelines and obligations will take precedence in the event of any uncertainty on a project's data management requirements.

5. The researchers' entitlement to be the first to publish based on data they have generated will be preserved.

[1] https://www.ukri.org/funding/information-for-award-holders/data-policy/common-principles-on-data-policy/

[2] https://www.ukri.org/files/legacy/documents/concordatonopenresearchdata-pdf/

6. It is recognised that types of data used, collected and generated will vary between disciplines and therefore the application of this policy will be sensitive to these differences while ensuring that best practice is promoted and funder requirements are met.

7. Researchers need to be aware of best practice measures for ***personal data*** collection, handling, security and sharing (including the appropriate deployment of anonymisation and related techniques and the creation of codebooks for their accompanying datafiles (e.g. a .txt file) so that data can be used/understood by third parties).

Research Data Management Policy

Before a project begins, a research Data Management Plan (DMP) must be completed

1. All research proposals must include a DMP that should be kept up-to-date as theproject progresses.

2. Plans should explicitly cover: ownership; standards/methodologies for data collection and management; ethical and privacy issues (including GDPR considerations if any personal data is involved); short-term storage and long-term preservation and/or deletion; data sharing and access/ temporary or long-term restrictions.

3. Where research is undertaken in partnership or under contract with a third party, a collaboration agreement must be signed before the start of the research that clearly addresses data ownership and partner responsibility for data storage.

Data collected during a project where the University is responsible for data storage must be stored on the University network, to ensure that it is suitably protected against accidental loss or damage and against unauthorised access

1. The University provides a secure Research Data Storage Service (RDSS) for this purpose, which ensures that only authorised staff can access project data, and that data can be restored in the event of accidental loss or damage.

2. Temporary use of portable devices and storage and/or the University's approved cloud service during, for example, field research, processing or collaboration must comply with the University's Data Storage Policy.

3. Data placed on temporary storage must be transferred back onto the RDSS as soon as the requirement for temporary storage has ended, to minimise the risk of reputational damage and/or litigation caused from lost, stolen or intercepted data.

4. Research proposals should consider whether storage requirements may exceed those currently offered by the University. Any such potential requirement should be discussed in advance of the application with both Information Services (infrastructure) and REIS (funding).

5. For datasets generated by simulation only the source code used to generate that data should be stored on the RDSS.

6. Before staff leave the university data of long-term value produced using University resources must remain accessible to the University.

7. Data containing personal information must be managed in accordance with the requirements of GDPR legislation and the document "Complying with GDPR at Abertay: Research Policy". The key points relating to management of personal data have been reproduced in the Appendix.

After a project, data with acknowledged long-term value must be preserved and made openly accessible, with as few restrictions as possible unless there are compelling reasons not to be so

1. At the completion of a project, the project lead must assess what data are of long-term value, and whether the data can be made openly available in a manner consistent with relevant legal, ethical and regulatory frameworks.
2. If research data are to be deleted or destroyed, this should be done in accordance with all legal, ethical and funder requirements and with particular concern for confidentiality and security.
3. Retained data suitable for external access should, where possible, be stored on a suitable national or international data service or subject domain repository (which may be specified by the funder).
4. If the funder does not specify a repository for data storage, and no suitable publisher, or discipline-specific archive is available, the University will provide a storage solution for long-term preservation and, if applicable, public access.
5. Data that supports published results must be preserved for 10 years from the date of publication of the findings, or longer if required by the funder.
6. Data that supports published results must be deposited no later than publication of the findings. Where the funder requires an earlier deposit, the timeframes specified by the funder take precedence.
7. In the case of research involving personal information, only anonymised data may be included in an open access dataset.

After a project, a metadata record describing retained data must be made publically available via Pure, within 12 months of the data being generated

1. A central catalogue of all preserved data will be published via Pure within 12 months of the data being generated (irrespective of where the data is hosted or whether it is publically accessible).

2. Metadata and documentation about research data should provide sufficient contextual information to enable the data to be discovered, accessed[3], understood, interpreted and reused by future users.

3. If access to the data is restricted, the published metadata should provide the reasons for the restrictions and summarise the conditions that must be satisfied for access to be granted.

Research publications must include a data access statement

1. A short statement must be added to research publications giving details of how data supporting the published results may be accessed (or explaining why access is restricted), along with an acknowledgment of any relevant funding body.

2. Metadata supporting publications should be accessible by the publication date and should be in citable form.

Management of non-digital data

In instances where analogue data is unsuitable for digitisation, all reasonable efforts must be made to ensure it is described in Pure, stored securely and organised in a manner that would facilitate the data being shared following receipt of a valid access request.

Use of others' data should always conform to legal, ethical and regulatory frameworks including appropriate acknowledgement

All users of research datasets should acknowledge the sources of their data and abide by the terms and conditions, under which they were accessed, in order to recognise the intellectual contributions of researchers who generate, preserve and share data.

*Data must always be managed, throughout its lifecycle, in compliance with all relevant legal, ethical, and regulatory frameworks**.***

Research data must be managed throughout its lifecycle in compliance with relevant legislation, and the following University policies covering: Intellectual Property; GDPR; Data Storage and Open Access Publications.

Responsibilities

Principal Investigators (PI) will:

1. Assume primary responsibility[4] for ensuring that data management activities comply with the requirements of this policy and with any relevant funders' policies.

[3] Via use of a robust and stable link to the data itself, where applicable, preferably in the form of a digital object identifier (DOI)>

[4] In the case of a PgR project, the supervisor will assume these responsibilities.

2. In the case of collaborative projects where the PI is based elsewhere, the lead researcher at Abertay must take responsibility for data generated at this University.

Researchers will:

1. Familiarise themselves with the requirements of this policy and with those of any funder(s) thereby assisting the PI to ensure that all data management activities are fully compliant.

2. Undertake all data management training provided by the University, and ensure that they are cognisant with the guidance and support available through the dedicated Research Data Management pages published on the Intranet.

The University will:

1. Ensure that appropriate training, support and advice is available to enable researchers to comply with this policy via the relevant professional support services.

2. Provide secure and backed-up storage for data during projects and provide advice on the most appropriate repository for long-term storage of completed and/or published datasets.

3. Provide a repository of "last resort" if no suitable external archive is available for the data to be deposited in. (Provision will cover cases where the data needs to be restricted and also cases where the data needs to be made discoverable and accessible).

4. Establish and maintain a central register of research records on Pure, listing all preserved datasets wherever they are hosted.

5. Further develop services that will support data management planning and decision making on issues related to data curation and retention, disposal and open access, in partnership with the research community.

Support

Guidance on Research Data Management is available via the University Intranet at https://intranet.abertay.ac.uk/research/data-management/ and for further advice please contact repository@abertay.ac.uk .

Appendix: Specific requirements relating to management of any data containing personal information and compliance with GDPR

1. Personal data should not be stored on cloud (external) services, such as DropBox.
2. Personal data should not be stored on unencrypted laptops or flashdrives.
3. Personal data should not be transferred via insecure channels, such as email.
4. Personal data should be stored no longer than necessary.
5. Data generated via online testing platforms must be transferred onto the RDSS as soon as the data file has been processed.
6. Consent forms must not be stored with data where they could compromise anonymization.
7. Non-Digital data must be stored in a locked laboratory/cabinet.
8. When working off campus the 'MyFiles' service should be used to access data held on the RDSS
9. If MyFiles cannot be used due to e.g. lack of network coverage then personal data can be temporarily transferred to a University provided encrypted USB.
10. Data placed on temporary storage must be transferred back onto the RDSS as soon as the requirement for temporary storage has ended.
11. Any 'keys' that could be used in combination with a data file to identify an individual should be shredded, as soon as possible upon project completion, if this key is no longer of use for the research project.

Further information on GDPR compliance, including the University's requirements for consent forms, anonymization, retention and timely disposal, audit trails and use of survey tools, can be found in ***Complying with GPDR at Abertay: Research Policy Document***