Newcastle University
Research Data Management Policy Principles & Code of Good Practice

This document outlines the overall policy of the University and its expectations of its staff and key services. More detailed practical help and information can be found on the 'Research Data Toolkit' website: http://research.ncl.ac.uk/rdm/

Policy Principles

1. The project Principal Investigator (PI) at Newcastle University has overall responsibility for the appropriate storage, treatment (including making data sets suitable for publication) and security of research project data. PIs may delegate discrete responsibilities to other members of the project team and this should be recorded.

2. All research projects are encouraged to create a data management plan at the earliest practical stage of a project. The plan should outline a project's approach to data, including costs and be reviewed regularly to ensure that practice remains in-line with expected standards.

3. All University staff are responsible for making themselves familiar with and adhering to legislation, funder guidance and University policy governing their research data.

4. The University expects that data (particularly personal data) be protected in line with both external and internal standards and discipline specific practice. The PI has responsibility for ensuring the safeguarding of personal identifiable research data and compliance with all relevant legal requirements.

5. Researchers should deposit all significant archive research data in an appropriate funder mandated or discipline specific data repository. Where this is not available, data should be deposited in an approved centre / manner.

6. Published datasets should be comprehensive and have clear instructions for access, which adheres to data citation principles. Metadata (descriptive information) should be rich enough to facilitate discovery, reproduction and reuse. Personal data should be protected in line with the University's Ethics Policy and Code of Good Practice.

7. Research data should remain available for 10 years following any publication (unless otherwise specified) after which retention will be reviewed. Metadata will be kept indefinitely.

8. Non-digital data or digital data that underpins a publication should be recorded in the University's data catalogue as a metadata record.

9. The University undertakes to provide appropriate resources, training, support and guidance to researchers and research support staff around data management and data governance. Where appropriate, the University will also provide a mechanism to record research metadata and to manage access.

10. Where research data has a commercial value or supports a commercial output such as a patent then public disclosure of the data may be delayed (this should be agreed in consultation with Research Strategy and Development).

Code of Good Practice in Research Data Management

1. Background & Purpose

The Policy Principles and Code of Good Practice have been written to guide researchers towards the best practice in the area of research data management. The document brings together guidance from across the institution and is designed as a single point of reference for academic and support staff. A research data management digital toolkit has been created to provide up-to-date links to related policies, funder requirements and best practice guidance. Collectively the policy principles, code of good practice and toolkit aim to:

- support good research data management practice
- ensure that data is handled appropriately
- maximise impact of open data by encouraging discoverability and reuse
- ensure compliance with legislation and funder polices
- protect sensitive / personally identifiable data
- protect intellectual property and commercialisation opportunities

The document sets out the best practice standards the institution expects of projects which it sponsors or which are undertaken in its name. It does not replace or override guidance from research funders; it should instead be considered as a complementary resource. If there are multiple guidelines then the most rigorous advice should be followed and / or advice sought from the Research Data Service (RDS).

2. Scope

The Policy and Code of Good Practice covers all funded research projects undertaken by Newcastle University staff and postgraduate researchers. The policy applies to all data (including active and archive data) regardless of format and relates to projects active at / from the time of policy approval.

The University acknowledges that a full implementation of this policy will be a long-term process.

3. Responsible Personnel / Bodies

Research Active Staff, Research Active Postgraduates, Research Data Service, Research Strategy and Development (including Legal & Joint Research Office), Library, IT Service, Head of Academic Units, University Research Committee, PIs, and Project Team Members.

3.1. Overall

University Research Committee (URC) has overall responsibility for the institution's research data strategy, its implementation and support. URC devolves responsibility for individual research projects to the project PI; however it recognises that for the PI to effectively perform their responsibilities they must be supported by other academic staff, academic units and the central services.

Responsibility for the implementation, operation and support of the policy as well as compliance to it is devolved to the Research Data Service (RDS). The RDS is also

responsible for reviewing the policy and ensuring it remains suitable for the requirements of the institution, funders and data providers.

3.2. Principal Investigators

Practical and operational responsibility for research data throughout the lifecycle of the project is in the hands of the project PI at Newcastle. Their key responsibilities are:

- ensuring data collection, storage, processing and dissemination are in line with legal and funder requirements
- ensuring project research data management maps to best practice in their research field
- delegating responsibility for research data management to other members of the project team e.g. to co-investigators or project administrators
- ensuring that the team / individual is competent (i.e. aware of their data management responsibilities and able to discharge them) and noting this in project documentation
- having in place a data management plan or appropriate project documents
- notifying the University of the location of and instructions on how to access archived research data
- including appropriate data access citations within their publications
- ensuring that data, should it be requested, is in an appropriate format e.g. anonymised and accessible

Should the Principal Investigator leave the University or no longer be able to continue in the role of being responsible for the project's data, a replacement should be appointed within the department/ research group.

In the case of student projects, the PI is the academic supervisor rather than the student themselves. The academic supervisor's is responsible for active data i.e. whilst the student is enrolled and archive data i.e. once the student has left.

3.3. Other Project Team Members

Are responsible for:

- discharging their responsibilities as delegated by the PI and detailed in the project documentation
- proactively supporting the PI with data management practice and raising any concerns to the PI in a timely manner

3.4. Research Data Service (RDS)

The Research Data Service (RDS) was established to provide support to researchers in managing their data and meeting the requirements of the University, funders and data providers. The RDS is a four-way partnership between the Library, Research Strategy and Development, University IT Service (NUIT), and Faculties.

Are responsible for:

- providing the guidance and support necessary to facilitate good practice in research data management
- providing advice and guidance on funder requirements
- provision of guidance regarding data security

- the provision of appropriate storage, back-up and where relevant the archiving of project data
- advising on the long term curation of research data outputs
- the technical support of the research information management systems
- providing guidance on the categorisation and classification of research output metadata (i.e. descriptive information relating to the data)
- co-ordinating the necessary training to enable faculties and academics to discharge their responsibilities
- advising on commercialisation
- acting as gatekeeper for any data access requests to University held data

3.5. Research Directors / Unit Managers

Are responsible for:

- the promulgation of the policy principles and code of good practice
- ensuring adherence to the policy principles in their unit
- where necessary establishing supplementary discipline specific guidance
- feeding information on researcher development and support requirements to Research Strategy and Development

4. Ownership of Data

Research data may have significant ethical, confidentiality, intellectual property, funder and legal restrictions attached to it and therefore ownership of the data should be established as early as possible. An appropriate agreement should be in place before the project starts. The Research Data Service will be able to advise and, where necessary, negotiate with funders on behalf of PIs.

Unless explicitly agreed the University owns the intellectual property rights, including copyright, to the research data created by researchers during the term of their employment with the University. Where research is externally funded this may create additional obligations and this should be taken into account.

Postgraduate research students will ordinarily own the intellectual property rights, including copyright, to the research data created during their studies. Exceptions exist where they are working on a funded project – please see the Research Student Confidentiality and IP Policy for further clarification. Nevertheless as the research sponsor the University requires that research students follow this policy, including the good data management and reuse aspects.

5. Use of Third Party Data

Where research involves usage of third party data, any terms and conditions associated with the data should be carefully scrutinised for potential copyright and / or licensing issues. These may have an impact on what data can be used for in the future. It is also important to ensure the data does not have any ethical restrictions associated with it e.g. it relates to non-anonymised personal identifiable data as this may affect the conditions of reuse.

6. Third Party Usage of University Data

Any data released for reuse should have a licence associated with its usage. This licence will ensure (at minimum) that the University and Academic Creator(s) are attributed in any

reuse of the data. The University will provide standard agreements which should be signed before data is shared. Access will be arranged through the Research Data Service.

Once data has been made available to the public, it should be noted that the data will then be available for further reuse. Therefore, the PI should ensure that the data is released at an appropriate point i.e. when opportunities for commercialisation and publication have been explored.

7. Sharing Data with Project Partners

A clear agreement regarding research data management and sharing should be put in place before any project start date. Special care should be taken where the project involves organisations outside the European Economic Area which may be governed by less robust legal frameworks and present a greater risk of unintended dissemination. Likewise when working with commercial organisations the increased intellectual property considerations should be taken into account when agreeing data sharing and publication. Research Strategy and Development will be able to assist in drawing up an appropriate agreement.

Details of data sharing; type, frequency, format and transfer arrangements should be noted within your data management plan and agreed at the project outset.

Links to Legal and Grants & Contracts

8. Commercialisation

Where research data has, or may have, commercial value, Research Strategy and Development should be consulted at the earliest possible stage. They will assist in assessing the value of the data, provide advice on the exploitation of any opportunities and whether publication of the data should be delayed or access restricted.

Link to Research Strategy and Development Policies and Enterprise Teams

9. Active Storage & Data Security

Each project should create and maintain a data management plan that details all key information on the project. For advice on this please see the additional resources.

Given the faculty based structure of the University, academic units are responsible for ensuring staff are aware of available options and use storage facilities that provide the required standards for their data. The Research Data Service will provide this information to the faculties.

Funded projects receive a data allowance of 0.5TB. Where project data needs are greater than this figure and funder requirements allow, additional resource should be costed into the project at the grant application stage.

For requirements outside of this please consult the Research Data Service (RDS) or the Institute IT Support Officer.

9.1. Digital Research Data

Wherever possible and appropriate data should be stored in digital format using approved storage systems. Data should be stored in a secure location, in a robust format, backed up

regularly and access to data should be controlled to protect against theft, misuse, damage or loss. Data should be stored according to best practice in the relevant field of research.

The IT Service provides a secure storage service; of which all staff receive a basic allowance and more can be requested although this may incur an additional cost. The IT Service can also provide guidance and advice on other external providers of data storage.

For information and guidance on the storage of digital data please see the IT Service (NUIT) and Governance web pages.

9.2. Non-digital Research Data

Wherever possible and appropriate non-digital research data should be digitised. If they cannot be digitised they should be stored securely in line with discipline best practice and digital metadata (information of data location and access conditions) provided at publication / project end.

10. Storage at Project End / Data Retention

The University mandates that the project data underpinning publications and data with acknowledged long-term value should remain accessible, and where appropriate discoverable, for at least 10 years.

10.1. Archiving

The responsibility for the archiving of the data lies with the PI and there are numerous national and data specific repositories. The PI should check that the sharing of the data is permissible and appropriate in light of confidentiality, ethical and legal concerns before depositing any data into a repository and making the data openly available.

10.2 Registration of Archived Data with the University

The University requires that the location of the data underpinning any publication be made available to the RDS (on request) if the funder requires or if the data is identified as being reusable.

11. Deletion

The University requires that the data is kept 10 years from the last date of access. After this point the data will be reviewed and either retained or destroyed. Any destruction will be in accordance with legal and funder requirements.

12. Breach(es)

Where a breach of this Policy and Code of Good Practice results in the unauthorised release of identifiable personal information into the public domain or non-compliance with external funder or regulatory requirements, this should be reported to the Research Data Service at the earliest possible time. If you are unsure whether a breach should be reported please contact the relevant Faculty Dean of Research Innovation.

The Research Data Service will then work with the Principle Investigator and project team to minimise any potential damage and to ensure that all relevant parties including participants, data providers and funders are appropriately advised.

Additional Resources

There are additional resources which support this document within the research data toolkit, these include:

- Relevant Policies
- Planning guidance and examples of data management plans
- Data storage and security
- Preservation and sharing guidance
- Training events and resources
- List of recommended repositories and storage providers
- Funder terms and conditions
- Information Governance Toolkit
- Contact details for relevant support

Policy Owner: Chris Emmerson, Research Data Manager, Research Data Service (Library)
Approved By: University Research Committee on 28 November 2016
Last Reviewed: University Research Committee in May 2018

Appendix A

Security-sensitive Research Material

Security-sensitive materials in this case can be defined as:-

a) Those which are covered by the Official Secrets Act (1989) and the Terrorism Act 2006.
b) Materials which could be considered 'extremist' or incompatible with British values.

The University supports both its academic faculty and student body in undertaking research utilising security sensitive materials but takes seriously its responsibility to protect them both from the potentially radicalising effects of viewing materials of this type and of misinterpretation of intent by authorities (which may result in legal sanction).

To ensure the University is able to protect its researchers it must be aware of the research before it begins. Early notification is through the ethical review process; it is from this that the institution is able to ensure proper data governance and oversight.

Ethical Review

The University is clear that research involving the access, collection and use of security-sensitive materials carries a risk to researchers as well as the general public and therefore any such research should go through full ethical review.

The University operates a two stage ethical review process for all its research. Within the preliminary stage, section six relates to data. The researcher should answer 'Yes' to the question.

1. Does the research involve the viewing, usage or transfer of Sensitive personal data as defined as by the Data Protection Act 1998, Terrorism Act (2006) or data governed by statute such as the Official Secrets Act, commercial contract or by convention e.g. client confidentiality? (If you are unsure please tick 'Yes' and complete the sub-questions).

Then answer 'Yes' to the relevant sub-question(s).

The researcher will then be directed to the full ethical review form where they will be asked to provide additional information on the types of data being used and materials accessed.

Data Governance

The downloading of (particularly terrorism related) security-sensitive materials and visiting of security-sensitive websites can be seen by the authorities as prosecutable offences should the intent behind them be illegal.

Research material which is security sensitive should not be kept on the researcher's personal computer or on their standard University drive. Before beginning the research, a member of NUITs Information Security Team should be contacted, they will arrange for the set-up of an appropriately secure project drive. Material within this drive will be easy to access but in some cases there will may restrictions preventing its exchange.

Likewise if the research involves visiting security-sensitive websites, the researcher should be aware that many of these sites are under surveillance by the authorities. It is strongly recommended that their University profile (IP address) is used to access these sites, thereby ensuring that their activities are flagged as being a legitimate part of their research and ensure that enquiries come to the institution in the first instance.

Physical data, e.g. manuals / reports should be scanned and a copy uploaded to the secure project file store.

By using a secure file store (along with appropriate ethics approval) the researcher will ensure that, should the University be asked, it can confirm that the materials within it are for research. Please be aware that in order to effectively answer any queries from the security services the Research Strategy and Development will be able to access metadata on the files e.g. titles and date of creation within the secure project drive. It will not however be able to access the content.

Oversight

The university also has a responsibility to ensure that researchers are not adversely affected (emotionally and intellectually) by the research they undertake. If there are any concerns these should be raised as soon as possible.

Student projects: In the first instance it is the project supervisor's responsibility to ensure that the students are not adversely affected. Supervisors should be prepared to liaise closely with the student's personal tutor and student welfare.

Staff projects: The Head of Unit will handle any concerns in consultation with Human Resources.

External Queries

Any queries from legitimate bodies e.g. the police or security services will be handled by the Research Strategy and Development in conjunction with the Information Security Team. If an individual receives an inquiry from the Police then the University's Research Strategy and Development tram should be advised of this.

The email contact for this and any other enquiries is res.policy@ncl.ac.uk