Guidance on the Research Data Management Policy

1 Definitions

1.1 **Research data** are the raw materials collected, processed and studied in the undertaking of research, and constitute the evidential basis that substantiates published research findings.

1.2 Research data may be primary data generated or collected by the researcher, or secondary data collected from existing sources and processed as part of the research activity.

1.3 Research data may be in digital or non-digital formats, and may include, but are not limited to: results of experiments or simulations, statistics and measurements, computational models and software, observational data, survey results, interview recordings and transcripts (and coding applied to these), images from cameras and scientific equipment, databases compiled from secondary sources, textual or linguistic corpora, lab books, and physical objects, such as samples and specimens.

1.4 **Research Data Management** (often abbreviated to RDM) encompasses the sum of activities undertaken by researchers and research organisations in relation to the collection, processing, retention and disposal of research data.

1.5 **Metadata** are structured information about a dataset in the form of a record documenting what the dataset is, how it was produced, who produced it, who owns it, where it is held, how and on what terms it may be accessed, and providing any other information that enables users to identify, interpret and use the data effectively.

1.6 **Researcher**: a researcher is anyone undertaking research or involved in collecting, generating or creating research data for or on behalf of the University, which shall include but not be limited to research staff, research students and visiting researchers.

1.7 **Data repository**: a data repository is any service that provides long-term preservation of and access to research data. Data repositories may be national or international services provided in support of defined disciplinary research communities, or institutional services based in research organisations.

1.8 **Access to information regimes** includes any statutory instrument that provides the right of access to information held by the University, e.g. the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Data Protection Act 1998.

2 The University's Research Data Management Service

2.1 The University undertakes to resource a Research Data Management Service for its research community, comprising technical infrastructure, systems and processes for the management, preservation and sharing of research data in accordance with funders' requirements, and will provide data management information, training and support services to researchers throughout the research lifecycle.

2.2 The website of the Research Data Management Service can be found here. The email contact address for the Service is reasearchdata@reading.ac.uk.

3 General responsibilities of researchers

3.1 All researchers have a responsibility to ensure that research data collected and processed in the course of their research activities are managed in accordance with the requirements of this policy, their funding bodies, and any legislative or contractual obligations that apply.

3.2 All researchers should have knowledge of relevant legislation, and should have completed all training as required by the University, including mandatory training for University employees in information security, Data Protection and Freedom of Information. University policies on **Data Protection**, **Freedom of Information**, **Copyright**, and **Information Security** are provided by Information Management and Policy Services here.

3.3 Furthermore, research data should be managed in accordance with the principles of research integrity set out in the **University Code of Good Practice in Research** (3.12) here.

3.4 Due consideration must be given to ownership of and rights in data generated by researchers. Where research is carried out under a grant or contract, the terms of the agreement will determine ownership and rights to exploit the data. Where no external contract exists, the University has ownership of data generated in the course of research undertaken by researchers in its employment and has a legitimate interest in protecting its intellectual property rights in the data. More information can be found in the **Code of Practice on Intellectual Property** here.

3.5 The ownership of IP in research data created by a student who is not an employee of the University rests with the student by default. However, IP in research data created by a student may be assigned to another party under the terms of a contract of sponsorship or employment. Students can also assign IP to the University, and in some conditions this may be required, as when there has been a significant contribution to the IP from a supervisor or other member of staff; or when the student has received significant financial support or material contribution from the University to undertake the research.

3.6 It is the responsibility of the Principal Investigator to ensure that research data management requirements specified by the University and any relevant funding bodies, and any legislative or contractual obligations, are observed during a research project or programme. Research data management roles and responsibilities should be clearly defined and documented within a research project.

3.7 All researchers involved in the handling of research data within a project should understand their roles and responsibilities in respect of such data, and should seek clarification of these from the Principal Investigator where necessary.

4 Planning research data collection

4.1 All new research proposals should address any requirements related to the collection and use of research data. This may be achieved by creating a data management plan that sets out what data will be collected in the course of the research, how the data will be collected and managed, how relevant data integrity, security, and confidentiality requirements will be met, what data will be retained after the conclusion of the research, what provisions for the sharing of data will be made (for example, through obtaining informed consent for sharing from research subjects), and how the data will be preserved for discovery and possible access by others.

4.2 Many funders require researchers to submit a data management plan addressing the proposed management, retention and sharing of research data as part of their grant application. Many public funders of research, including all of the UK Research Councils, accept that management of research data is a legitimate research expense. More information on the requirements of funders and preparation of data management plans is provided by the Digital Curation Centre here.

4.3 Technical support requirements for the collection, storage and processing of research data should be considered at the planning stage. Information about data storage and other support for the management of research data provided by IT Services can be found in the IT Service catalogue under File Storage (login required). General information on preparing grant applications is provided by Research and Enterprise Development here.

4.4 Where research is undertaken in partnership or under contract with a third party, issues of data ownership, the University's obligations under the access to information regimes and intellectual property rights should be addressed at the outset, in order to avoid disagreement or confusion at a later stage.

4.5 The University accepts that in collaborative research the ownership of and rights in research data may be subject to the terms of any partnership agreement, and that third parties may have a legitimate interest in controlling the outputs of a research project. Where possible, any agreement should recognise the broad objectives of this policy, including the intellectual property interests of the University, and should allow for the wider sharing of research data within a reasonable period of time after completion of the research.

4.6 Where data are to be collected from human subjects, planning should consider whether consent for wider sharing of the data may be obtained, and anticipate such processing as may be necessary to enable sharing of data after completion of research. Collection of personal or sensitive data need not be inconsistent with data sharing, provided researchers use appropriate strategies of informed consent, anonymisation, and controlled access where relevant. More information is provided by the UK Data Service here.

4.7 Where secondary data owned or controlled by a third party are collected and processed for the purpose of research, researchers should consider any need to make the processed data available in support of anticipated research findings, and where necessary seek permission to reproduce the data. More information is provided by the UK Data Archive here.

5 Managing research data

5.1 Research data collected and processed in the course of research should be handled by designated members of the research team in accordance with documented protocols. The use of defined procedures for data storage and backup, file naming and organisation, version control and metadata creation will increase the efficiency of the research process, safeguard against corruption or loss of data, and make it easier to prepare data for retention and sharing at the end of the project.

5.2 Researchers should use University-approved storage and regular backup procedures, in order to guarantee the security and integrity of research data and protect against loss or corruption. Research data must be processed in accordance with the University's information security policies; in particular personal and sensitive data must be securely managed in accordance with the **Encryption Policy**, which can be found here.

5.3 Researchers are strongly advised not to rely exclusively on the hard disk drives of PCs or on non-networked devices such as removable drives or USB sticks for the storage of data. Where such storage solutions are used, data saved to them should be backed up regularly to secure storage.

5.4 Non ITS-authorised third party hosting services such as Dropbox may provide useful solutions for remote access to data or sharing with collaborators, but should be used with caution, as their security cannot be guaranteed. They should never be used for sharing or processing unencrypted personal or sensitive data, nor should they be used as the primary or sole copy of research data.

5.5 Non-digital data should be organised, documented and stored securely. If the data contain personal or sensitive data they must be stored and processed securely in accordance with the **Data Protection** and **Information Security** polices, which can be found here.

6 Retention, sharing and disposal of data

6.1 Relevant research data should be made available for access and re-use by other researchers within a reasonable length of time after the completion of research, providing there is no legal, ethical or commercial reason why this should not be done. This is in accordance with the **Information Framework** Principle 3, on Open access and use, which encourages a culture of openness and transparency around the information the University holds. The **Information Framework** can be consulted here.

6.2 All researchers are entitled to a limited period of privileged use of the data they have collected to enable them to publish the results of their research. The length of this period may be determined by the policy of any research funder, but in principle data supporting research findings should not be withheld later than the date of first publication of research results, except where there is an overriding legal, ethical or commercial reason why the data cannot be released.

6.3 Data that substantiate research findings should be offered for deposit and preservation in a suitable data repository, and any publication based on the data should include a statement indicating where and on what terms the data may be accessed.

6.4 Not all data collected in the course of research need be retained after completion of the research. Research data may go through several stages of processing during a research project, and much of these data will be unsuitable for retention. Data should be retained that directly underpin published findings, with enough descriptive metadata to enable other users to understand how the resultant dataset was produced. It may also be desirable to retain other data that are deemed to have long-term value.

6.5 Retained data should be stored in a form that would enable retrieval by a third party for a minimum of three years, or for a longer period according to the requirements of the funding body or any other legal, ethical or contractual requirements that apply.

6.6 Many public funders of research specify what data should be retained and shared, when the data should be shared, and the minimum period for which they should be retained. Funders may require researchers to preserve supporting data for a minimum of ten years after the completion of research, and in some cases for considerably longer. Funded researchers must observe the conditions of their grants in respect of data preservation and sharing.

6.7 Data may be legitimately withheld where personal or sensitive data have been obtained for a specific research purpose under conditions of confidentiality, or where consent for sharing of data has not been given, or where other legal or ethical considerations apply.

6.8 Where confidential or sensitive data have been collected and it is possible to share them in some form, for example through processes of anonymisation and aggregation, or through granting access to authorised persons under non-disclosure agreements, the data should be prepared and licensed for access using relevant processes.

6.9 Preserved data should be subject to review on expiry of the mandated period of retention, and a decision should be made at this time either to retain the data for a further fixed period or to dispose of the data if there is no longer any reason for them to be preserved.

6.10 When a dataset has been deposited in a data repository or otherwise stored for preservation, the researcher should register the details of the dataset with the University, even if access to the data is restricted, so that a record of the data can be maintained and made available for discovery.

6.11 To register a research dataset, contact the Research Data Management Service at researchdata@reading.ac.uk with the following details: the name of the dataset; who created and is responsible for the dataset; the location where the dataset is stored; and the terms under which the dataset may be accessed. It is sufficient to provide a DOI or other persistent identifier linking to the full dataset if one has been assigned.

6.12 Where research data are not retained they should be disposed of according to University guidelines. Particular care should be taken in the disposal of personal and sensitive data. Further guidance is available here.