

University Guide to Research Data Management

UPR IM16 Appendix III version 05.0

Policies superseded by this document

This document replaces version 04.0 of UPR IM16, with effect from 3 January 2023.

Summary of significant changes to the previous version

Links and UPR references have been updated.

Glossary

A glossary of approved University terminology can be found in [UPR GV08](#).

Table of contents

1	Introduction	1
1.2	Why manage research data?	2
2	Context.....	2
2.4	External funding requirements	3
2.5	Consultation process.....	3
2.6	Security-sensitive research material.....	3
3	Definition	4
3.1	Classification of research data	4
4	Data Management Plan.....	4
5	Creating the Data Management Plan.....	5
5.2	Checklist for a Data Management Plan	5

1 Introduction

- 1.1 This Guide to Research Data Management was approved by the Chief Executive’s Group on 6 June 2011 and sets out the arrangements for meeting the University’s data management requirements set out in UPR IM16¹ and for completing the data planning elements of funding bids.

¹ UPR IM16 ‘Data Management Policy’

1.2 Why manage research data?

“To maintain research integrity (and protect their reputations), institutions and researchers must ensure research data are preserved so that results can be verified and the data reused in future. Re-use maximises the return on public investment in research.

(JISC: <https://www.jisc.ac.uk/guides/rdm-toolkit>)”

By managing their data researchers and others with responsibility for research data management will:

- a meet legal and funding body grant requirements;
- b ensure research integrity and replication;
- c ensure research data and records are accurate, complete, authentic and reliable;
- d increase research efficiency;
- e save time and resources in the long run;
- f enhance data security and minimise the risk of data loss;
- g prevent duplication of effort by enabling others to use the data;
- h comply with practices in industry and commerce;
- i enable the effective re-use of research data;
- j enable freely available public access to research data outputs in accordance with national and funding body policies and to enhance the University’s wider research profile.

2 Context

2.1 These guidelines should be read in conjunction with section 7 (‘Research Data’), UPR IM16¹ and with UPR RE02² (‘Research Misconduct’) which defines research misconduct as (amongst other things) the fabrication, falsification, corruption of and/or failure to preserve research data.

2.2 Where access to data is granted to any third party or where data are routinely shared between the University and any third party, reference must be made to the Template [Data Sharing Agreement](#)³ (see Appendix IV, UPR IM08⁴).

² UPR RE02 ‘Research Misconduct’

³ [http://www.studynet2.herts.ac.uk/ptl/common/ict.nsf/0/7391EBE5D088780E802577EC004C58B0/\\$FILE/Data Access Agreement.pdf](http://www.studynet2.herts.ac.uk/ptl/common/ict.nsf/0/7391EBE5D088780E802577EC004C58B0/$FILE/Data%20Sharing%20Agreement.pdf)

⁴ Appendix IV, UPR IM08 ‘Template Data Sharing Agreement’

2.3 Reference must also be made to Appendix II, UPR IM16⁵, which applies to the processing, creation, use, disclosure, dissemination and storage of person-identifiable data and other confidential and commercially sensitive data and documents (termed Personal and Confidential Information (PCi)). Appendix II, UPR IM16⁴ sets out how PCi can process safely. The guidance set out in this document (Appendix III, UPR IM16), supports the policies and principles set out in the University's Information Management Principles (UPR IM02⁶), the IT and Computing Regulations (UPR IM20⁷) and the Records Management Standards set out in UPR IM11⁸.

2.4 External funding requirements

These Guidelines (Appendix III, UPR IM16) will help answer questions set out by external funding bodies relating to management and the sharing of data.

2.5 Consultation process

It is the responsibility of the Principal Investigator, as Data Steward, to consult at an early stage with the Research Grants Team, Business and Research Office, about funding bids and with their designated Knowledge and Business Intelligence Consultant (KBIC) in Information Hertfordshire about their Data Management Plan (DMP), including any technical requirements.

2.6 Security-sensitive research material

2.6.1 Universities play a vital role in carrying out research on issues where security-sensitive material is relevant. If circulated carelessly, such material is sometimes open to misinterpretation by the authorities, and can put authors in danger of arrest and prosecution under, for example, counter-terrorism legislation. Universities UK (UUK) publishes guidance to researchers on good practice to be followed at: <https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2019/Oversight-security-sensitive-research-material-guidance-3.pdf>

2.6.2 Any researcher, staff or student, who, for the purposes of their research, needs to access or store materials that may be considered sensitive under Obscene Publications, Counter-Terrorist or other relevant legislation, must obtain the prior written consent to such access from the Director of the Doctoral College who may not delegate this responsibility. In this regard, the Director of the Doctoral College acts as the Institutional Lead for Research Integrity and nominee of the Secretary and Registrar, from whom such consent must be sought in the absence of the Director of the Doctoral College. The Director of the Doctoral College will ensure that a record is kept of all consents so given. Researchers to whom such consent is given will comply with all relevant regulations and guidelines to ensure the safe and secure storage of any material accessed and will comply with any conditions imposed on access by the Director of the Doctoral College.

⁵ UPR IM16, Appendix II 'Managing Personal and Confidential Information'

⁶ UPR IM02 'Information and Data Management Principles'

⁷ UPR IM20 'IT and Computing Regulations'

⁸ UPR IM11 'Records Management and the Archiving and retention of Prime Documents and Business Records'

3 Definition

Research data, unlike other types of information, are collected, observed, or created, for purposes of analysis to produce original research results.

3.1 Classification of research data

3.1.1 “Research data can be generated for different purposes and through different processes (Research Information Network classification 2007):

- i **Observational:** data captured in real-time, usually irreplaceable. For example, sensor data, survey data, sample data, neuroimages.
- ii **Experimental:** data from lab equipment, often reproducible, but can be expensive. For example, gene sequences, chromatograms, toroid magnetic field data.
- iii **Simulation:** data generated from test models where model and metadata are more important than output data. For example, climate models, economic models.
- iv **Derived or compiled:** data is reproducible but expensive. For example, text and data mining, compiled database, 3D models.
- v **Reference or canonical:** a (static or organic) conglomeration or collection of smaller (peer reviewed) datasets, most probably published and curated. For example, gene sequence databanks, chemical structures, or spatial data portals.”

4 Data Management Plan

4.1 A Data Management Plan ensures that all aspects of data management are fully perceived at the start of a project. A Data Management Plan is a document which describes:

- a what research data will be created;
- b what policies (funding, institutional and legal) apply to the data;
- c who will own and have access to the data;
- d who will be responsible for each aspect of the Plan;
- e how its re-use will be enabled and long-term preservation ensured after the original research is completed;
- f what data management practices (backups, storage, access control, archiving) will be used and, therefore, what facilities and equipment will be required;
- g the resources required for the management and use of the research data.

4.2 The Data Management Plan must be maintained continuously and kept up-to-date throughout the course of research.

4.3 A Data Management Plan must be completed for every research project as follows:

- a if a Data Management Plan is required by the funding body, the Data Management Plan must be completed at the **bid application stage**;
- b if a Data Management Plan is not required as part of the bid application, then a Data Management Plan must be completed **once the award is made and before the start of the research project**.

5 Creating the Data Management Plan

5.1 To create a Data Management Plan, researchers are advised to follow the steps set out in this section (5).

- a Check whether the Data Management Plan is required at the funding bid application stage or when the award is made (see section 4.3).
- b Complete and save a Data Management Plan using the online tool available at <https://dmponline.dcc.ac.uk>. This offers a convenient and efficient way of creating a Data Management Plan which addresses all the requirements.

5.2 Checklist for a Data Management Plan

5.2.1 For further information refer to the checklist available from the National Digital Curation Centre at <https://www.dcc.ac.uk/DMPs/Checklist>.

5.2.2 The Checklist consists of the following main headings and subheadings for consideration when drawing up a Data Management Plan:

- i **Introduction and Context:**
for example, funding body, duration, partner organisations.
- ii **Data Types, Formats, Standards and Capture Methods:**
for example, existing data sets to be used; file naming conventions; metadata standards (Ensure that University of Hertfordshire file naming conventions are used as set out in UPR IM11⁸).
- iii **Ethics and Intellectual Property:**
for example, issues preventing sharing of data, personal and confidential information, IPR considerations.
- iv **Access, Data Sharing and Reuse:**
for example, is data sharing required by the funder, process for access, when/how data can be exploited, licensing?
- v **Short-Term Storage and Data Management:**
for example, location of data, back-ups, security, access during the project's lifetime.
- vi **Deposit and Long-Term Preservation:**
for example, the basis for keeping data over the longer term, retention schedule, data archive/repository and metadata for discovery, managing sensitive data access, licensing etc.
- vii **Resourcing:**
for example, staff roles/responsibilities, how data management is to be funded during the lifetime of the project and beyond?
- viii **Adherence and Review:**
for example, how/when and by whom the data management plan will be reviewed?
- ix **Agreement:**
for example, statement of agreement.

- 5.2.3 Seek advice and guidance from their Information Manager.
- 5.2.4 Send a copy of the completed Data Management Plan to the Chief Information Officer for retention as the official University record.
- 5.2.5 Update the Data Management Plan as required throughout the research project.

Sharon Harrison-Barker
Secretary and Registrar
Signed: **3 January 2023**

Alternative format

If you need this document in an alternative format, please email us at governanceservices@herts.ac.uk or telephone us on +44 (0)1707 28 6006.