Title	Data Management Policy – **IM16**
Version	04.0
Effective	13 December 2019

DATA MANAGEMENT POLICY

General changes	
Additional requirements regarding security-sensitive research material have been added to Appendix III. Links and references to other UPRs have also been updated as required.	
Section	
1.2,iv	List of UPRs updated
1.3	Reference to Appendix IV, UPR IM16 deleted
Appendix III, section 2.3	See text
Appendix III, section 2.6.2	Link updated
Appendix III, section 2.6.2	Paragraph added

---

*(Amendments to version **03.1**, UPR IM16 are shown in italics.)*

Structure

	APPENDICES:
	APPENDIX I – Master Sources with Assigned Data and Document Steward Responsibilities (link to intranet)
	APPENDIX II – Cyber Security and Managing Personal and Confidential Information (link to intranet)
	APPENDIX III – University Guide to Research Data Management

1 INTRODUCTION

1.1 The University operates in an increasingly complex, data-oriented, environment which requires the effective collection, management, analysis and dissemination of data. The data generated and held by the University are key assets that must be managed correctly to underpin University strategic development, essential functions and academic integrity.

1.2 This document:

i provides a corporate framework with defined roles and responsibilities for the collection, quality, storage, security, maintenance and dissemination of institutional data;

ii has as its basis the Key Principles set out in UPR IM02[1];

iii has been approved by the Chief Executive's Group[2];

iv should be read in conjunction with UPR IM02[1] and UPR IM11[3] and the following related regulatory documents: UPR IM*20*[4]; UPR IM08[5]; UPR IM09[6]; UPR CA04[7] and UPR RE02[8].

(**Note for guidance:**

Other related documents include 'University Guidance for Managing Personal and Confidential Information', 'Staff Computing Guide', and 'University instructions for downloading and using TrueCrypt encryption'.)

1.3 UPR IM16 consists of the following:

Data Management Policy (UPR IM16)

Master Sources with Assigned Data and Document Steward Responsibilities (Appendix I, UPR IM16) – internal access only, refer to https://www.herts.ac.uk/about-us/governance/university-policies-and-regulations-uprs/uprs/information-management-and-systems

Managing Personal and Confidential Information (Appendix II, UPR IM16) – internal access only, refer to https://www.herts.ac.uk/about-us/governance/university-policies-and-regulations-uprs/uprs/information-management-and-systems

University Guide to Research Data Management (Appendix III, UPR IM16)

---

1 UPR IM02 'Information Management *Principles*'
2 Chief Executives Group, 26 April 2010
3 UPR IM11 'Records Management and the Archiving and Retention of Prime Documents and Business Records'
4 UPR IM*20 'IT and Computing Regulations'*
5 UPR IM08 'Data Protection'
6 UPR IM09 'Freedom of Information'
7 UPR CA04 'Commercial Activities'
8 UPR RE02 'Research Misconduct'

2 DEFINITIONS

2.1 For the purposes of this document the following definitions will apply:

2.1.1 **'data'**:

distinct units of information such as facts, numbers, letters, symbols, usually formatted in a specific way, stored in a database and suitable for processing by a computer;

2.1.2 **'Data Dictionary'**:

a file that defines the basic organisation of a database, containing a list of all files in the database, the number of records in each file and the names and types of each field;

2.1.3 **'Data Management Framework'**:

the organisational structure in place to manage the University's data assets (section 6, refers);

2.1.4 **'data quality'**:

the accuracy, completeness, validity and currency of the data;

2.1.5 '**Dataset**':

a defined collection of data with common elements related to a specific function;

2.1.6 **'Data Steward'**:

the Head of the Strategic Business Unit or other Officer responsible on behalf of the University for the collection, management and use of data;

2.1.7 **'Data Expert'**:

the person responsible for the operational management and processing of the data in an information system who has detailed knowledge and experience in the operational management and use of specific Datasets and their structures, capture, administration, processing and reporting;

2.1.8 '**Data User**':

an individual authorised to access and use data;

2.1.9 **'Information'**:

data combined and processed into a meaningful form;

2.1.10 **'Information system'**:

a computer system used to gather, store, structure, secure, process, combine and filter data into information and that makes that information available on time and in a useful form for users and institutional requirements.

3 SCOPE

3.1 The University's Data Management Policy applies to:

i data, in all its forms, required for the management and administration of the University and the conduct of its work, whether the data are captured and accessed from on-campus or off-campus locations;

ii all University of Hertfordshire activities;

iii individual Members of the University (UPR GV06[9], refers);

iv the University's wholly-owned subsidiary companies and their wholly-owned subsidiaries subject to the approval of their respective Boards of Directors;

v collaborative activities undertaken with Partner Organisations;

vi the management of research data.

(**Note for guidance:**

The principles of the Data Management Policy (UPR IM16) also apply to document management and use. Refer to (UPR IM11[3] for further information about University Records Management.)

4 POLICY

4.1 All data created or owned by the University, its wholly-owned subsidiary companies and their wholly-owned subsidiaries, are the property of the University of Hertfordshire Higher Education Corporation and are regarded as corporate assets.

(**Notes for guidance:**

- These data include, but are not limited to, data relating to management and administration and to the conduct of the University's business.
- Although responsibility for research data may be vested elsewhere, it should be noted that this policy and the principles and standards that it defines also apply to the **management and use** of research data (section 7, refers).)

4.2 The University recognises the value of data as an institutional resource and considers that value to be increased through the widespread and appropriate use of data and by virtue of data quality.

4.3 The University considers the value of data to be diminished through misuse, misinterpretation or unnecessary access restrictions.

4.4 Access to data will be granted to Data Users for all legitimate University purposes, subject to any limited access restrictions that may be determined from time-to-time at the absolute discretion of the University.

(**Note for guidance:**

Data access is determined on behalf of the University by the Chief Information Officer.)

4.5 The University is committed to the Data Management Standards set out in section 5 of this document.

---

[9] UPR GV06 'Membership of the University'

5 DATA MANAGEMENT STANDARDS

5.1 The University categorises and determines data access as follows:

5.1.1 **'University Internal'**

Data categorised as 'University Internal' may be accessed by all Data Users, without restriction.

(**Note for guidance:**

'University Internal' is the default category for all data.)

5.1.2 **'Limited Access'**

i At the absolute discretion of the University, specific data may be categorised as 'Limited Access'.
ii Date will be categorised as 'Limited Access' by the Chief Information Officer in light of recommendations from Data Stewards and, where appropriate, legal and other advice.

(**Note for guidance:**

The grounds for categorising data as 'Limited Access' include, but are not limited to, personal privacy, legal requirements, commercial confidentiality, security, externally imposed constraint or other recognised good reason.)

5.1.3 **'Public Access'**

i Data which, at the absolute discretion of the University, are determined to be a matter of public record and can, therefore, be made freely available, without restriction, are categorised as 'Public Access'.

ii Date will be categorised as 'Public Access' by the Chief Information Officer in the light of recommendations from Data Stewards, Freedom of Information requirements and, where appropriate, legal and other advice.

5.2 **Data Stewards**

(Section 6.5, also refers.)

5.2.1 Every data source and Dataset must have a designated Data Steward.

5.2.2 Data Stewardship of a Dataset will be delegated to the Head of Strategic Business Unit or other Officer with primary responsibility for the University operations to which the Dataset relates.

5.2.3 A Data Steward is responsible for the data quality, security and availability of the data for which he or she is Data Steward.

5.3 **Data Experts**

(Section 6.6, refers.)

Data Experts are responsible for and accountable to the relevant Data Steward for:

a the operational management of the assigned institutional data and its integrity;
b applying University data management standards and procedures;

c effective liaison with the technical experts responsible for the repositories where the data are stored and for the applications and reporting systems for use of the data;
d data analysis;
e providing management information to support University decision-making;
f external reporting requirements;
g resolving queries;
h implementing agreed data retention criteria and archiving policies;
i making the Data Dictionary understandable to users.

5.4 **Data Users**

(Section 6.7, also refers.)

5.4.1 Subject to any data access restrictions determined on behalf of the University by the Chief Information Officer, permission to access data will be granted to:

a all staff for legitimate University purposes and
b other individuals, where agreed, following the conduct of a University Data Access Authorisation process.

5.4.2 Data Users are required to:

a access and use data only in their conduct of University business;
b access only the data needed to carry out their University work;
c respect the confidentiality and privacy of individuals whose records they may access;
d observe any ethical, commercial, security or other restrictions determined by the University that apply to the data to which they have access;
e comply with all relevant legal requirements;
f comply with the Data Management Standards (section 5, refers);
g work within the limits of the data access that they have been granted.

5.5 **Data**

5.5.1 Data:

a must be readily available to all Data Users with a legitimate University business need through easily accessible web-based interfaces;
b must be stored in an official University data repository agreed with the Chief Information Officer (or nominee);
c should be defined consistently across the University;
d element names, formats and codes must be consistent across all repositories and information systems that use the data and consistent with any agreed University standards;
e should, wherever possible, be captured or entered once only;
f structures must be under strict change control so that business and system implications of any change can be properly managed;
g for data capture, validation and processing should, wherever possible, be automated;
h updating processes should be standard across the University and its systems;
i should be recorded in an auditable and traceable manner and in accordance with any agreed change control processes;
j should not be duplicated unless duplication is absolutely essential and has the approval of the relevant Data Steward; in such cases, one source must be clearly identified as the master and there must be a robust process to ensure copies are not modified and are kept in step with the master source;
k exchange protocols between data repositories must be under strict change control so that business and system implications of any change can be properly managed.

5.5.2 Arrangements for the storage and use of limited access data and any third party use of the data must conform with Appendix II, UPR IM16[10].

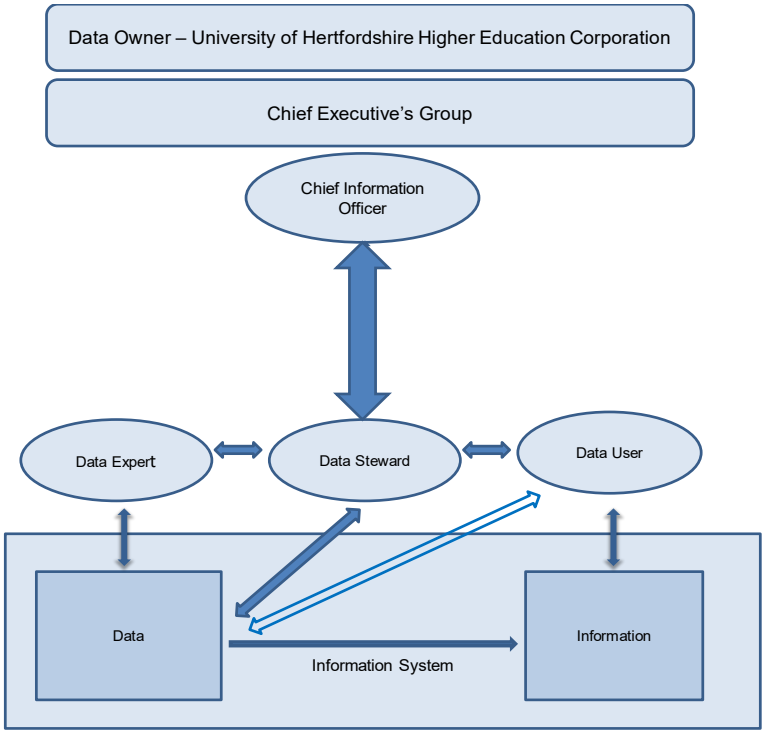
5.5.3 Whenever possible, international, national or industry standards for common data models must be adopted. When this is not possible, institutional standards will be determined.

6 DATA MANAGEMENT FRAMEWORK

(Appendix I, UPR IM16[11], refers.)

6.1 The following structure forms an institutional Data Management Framework, the purpose of which is to ensure data are consistent, of good quality and available for use by Data Users.

6.2 Data Management Framework



6.3 Data Owner

The University of Hertfordshire Higher Education Corporation.

6.4 Chief Information Officer

6.4.1 The Chief Information Officer is responsible:

a to the Vice-Chancellor, through the Chief Executive's Group, for data owned and managed by the University of Hertfordshire Higher Education Corporation;
b for data management policy, standards and procedures;
c for the University's data model, its promotion and its implementation;

---

10 Appendix II, UPR IM16 'Managing Personal and Confidential Information';

11 Appendix I, UPR IM16 'Master Sources with Assigned Data and Document Steward Responsibilities'

d for monitoring and reviewing the effectiveness of data management policy, standards and procedures;
e formulating data management policy and standards for the approval of the Chief Executive's Group;
f advising the Chief Executive's Group on their implementation;
g establishing procedures for the management of and access to data;
h overseeing the implementation of and compliance with data management policy, standards and procedures;
i adjudicating on any disputes that may arise from time-to-time;
j in conjunction with Data Stewards, reviewing annually, the Data Management Policy (UPR IM16).

6.5 **Data Stewards**

6.5.1 Data Stewards are responsible for and accountable to the Chief Information Officer for:

a the management of the assigned institutional data;
b co-ordination of the associated Data Experts;
c the collection and updating of the assigned institutional data;
d recommending changes to institutional data management policy and procedures;
e data quality;
f the implementation of Data Management Standards and procedures;
g the promotion of the management of University data as a vital corporate resource;
h understanding and promotion of the value of data for University-wide purposes and facilitation of data sharing and integration;
i authorisation and management of any third party use of the data in accordance with University policies and processes;
j liaison with other Data Stewards as required;
k advising and reporting on data management issues to the Chief Information Officer.

6.6 **Data Experts**

6.6.1 Data Experts are responsible for and accountable to the relevant Data Steward for:

a the operational management of the data assigned to them and its integrity;
b applying University data management standards and procedures;
c effective liaison with the technical experts responsible for the repositories where the data are stored and for the applications and reporting systems for use of the data;
d data analysis;
e providing management information to support University decision-making;
f external reporting requirements;
g resolving queries;
h implementation of agreed data retention criteria and archiving policies;
i making the Data Dictionary understandable to users.

6.7 **Data Users**

6.7.1 Data Users are responsible for and accountable to their managers for:

a ensuring their use of the data complies with this policy (UPR IM16) and all related standards and procedures;
b for all data access made through their user account and the subsequent use and distribution of the data;
c identifying any potential personal conflicts of interest resulting from the authorised data access granted to them through their user account (including potential conflicts of interest where the data user is both a member of staff and student of the University) and for seeking advice from the relevant Data Steward;

d for obtaining permission from the Data Steward for use of the data for marketing campaigns or other contact list purposes;
e for contributing to the accuracy and integrity of the data through the timely correction and updating of data where authorised to do so and for other data, through timely notification to the relevant Data Steward.

6.7.2 Data users must:

a not disclose their user login account password to anyone;
b not use data for their own personal gain or for the gain or profit of others;
c not access data for personal business purposes or personal interest;
d not disclose data to unauthorised persons or to any third party without the consent of the relevant Data Steward;
e not disclose data about an individual to another person, regardless of that person's relationship with the individual concerned, without the consent of the individual concerned and/or without the consent of the relevant Data Steward;
f present the data accurately and objectively in any use that is made of it.

7 RESEARCH DATA

(Appendix III, UPR IM16[12], refers.)

7.1 Data management is an essential and integral part of the responsible conduct of research.

7.2 The University is responsible for:

i ensuring effective data management to meet internal and external requirements, including enabling the re-use of research data and freely available public access to research data outputs in accordance with national and funding body policies;

ii retention of research data in sufficient detail for a defined period to enable appropriate responses to any questions about accuracy, authenticity, primacy and compliance with legal and regulatory requirements governing the conduct of research;

iii for supporting investigation into any allegations of misconduct or regulatory breach (UPR RE02[13], refers).

7.3 This policy and the principles and standards that it defines also apply to the management and use of research data.

7.4 Data Steward - research data

For the purposes of research data, the Principal Investigator or agreed equivalent role (such as the Principal Supervisor of Research Students) shall fulfil the role and responsibilities of the Data Steward for the purposes of the collection, management and retention of research data.

(**Note for guidance:**

For further information refer to 'University Guide to Research Data Management' (Appendix III, UPR IM16[16], refers).)

8 REVIEW ARRANGEMENTS

This Data Management Policy (UPR IM16) and the arrangements for its implementation will be reviewed annually by the Chief Information Officer in conjunction with the Data Stewards.

---

12 Appendix III, UPR IM16 'University Guide to Research Data Management'
13 UPR RE02 'Research Misconduct'

APPENDIX III – UNIVERSITY GUIDE TO RESEARCH DATA MANAGEMENT

Structure

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 IM16[14] and for completing the data planning elements of funding bids.

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/research-data-management*)"

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 IM16[1] and with UPR RE02[15] ('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 (Appendix IV, UPR IM*08*[16], refers).

---

14 UPR IM16 'Data Management Policy'
15 UPR RE02 'Research Misconduct'
16 Appendix IV, UPR IM*08* '*Template* Data Sharing Agreement'

2.3 Reference must also be made to Appendix II, UPR IM16[17], 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 IM16[4] 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 IM02[18]), the *IT and Computing Regulations* (UPR IM*20*[19]) and the Records Management Standards set out in UPR IM11[20].

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 his or her 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.*

---

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

18 UPR IM02 'Information Management *Principles*'

19 UPR IM20 '*IT and Computing Regulations*'

20 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 (section 4.3, refers).

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 http://www.dcc.ac.uk/webfm_send/431 .

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 IM11[7]).

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.

Sue Grant
Secretary and Registrar
Signed: **13 December 2019**