

Data Management Policy

UPR IM16 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Policies superseded by this document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

Amendments have been made in line with changes to UPR IM02 'Information and Data Management Principles' (e.g. section 2, 'definitions'). Data access categories have been renamed (see section 5) and a new section of 'unstructured data' has also been added (section 7).

Glossary

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

Table of contents

1	Introduction	2
2	Definitions	3
3	Scope	3
4	Policy	3
5	Data Management Standards	4
5.1.1	'Internal'	4
5.1.2	'Confidential' or 'Highly Confidential'	4
5.1.3	'Public'	4
5.2	Information Asset Owners	5
5.3	Data Experts	5
5.4	Data Users	5
5.5	Data	6
6	Data Management Framework	6
6.2	Data Management Framework	7
6.3	Data Owner	7
6.4	Chief Information Officer	7
6.5	Information Asset Owners	8
6.6	Data Experts	8
6.7	Data Management Group	8
6.8	Data Users	9
7	Unstructured Data	9

8	Research Data	10
8.4	Information Asset Owner - research data	10
9	Review Arrangements	10

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 IM02¹;
- iii has been approved by the Chief Executive's Group²;
- iv should be read in conjunction with UPR IM02¹ and UPR IM11³ and the following related regulatory documents: UPR IM20⁴; UPR IM08⁵; UPR IM09⁶; UPR CA04⁷ and UPR RE02⁸.

(Note for guidance:

Other related documents include 'University Guidance for Managing Personal and Confidential Information' and 'Staff Computing Guide'.)

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 \(link to intranet\)](#)

Managing Personal and Confidential Information (Appendix II, UPR IM16) – [internal access only \(link to intranet\)](#)

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

1 UPR IM02 'Information and Data 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 IM20 'IT and Computing Regulations'
 5 UPR IM08 'Data Protection and Privacy Statement'
 6 UPR IM09 'Freedom of Information'
 7 UPR CA04 'Commercial Activities'
 8 UPR RE02 'Research Misconduct'

2 Definitions

For the purposes of this document the definitions in UPR IM02 'Information and Data Management Principles' will apply.

3 Scope

3.1 The University's Data Management Policy applies to:

- i data, in all its forms - structured or unstructured -, 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 (see UPR GV06⁹);
- 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 IM11³ 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 (see section 7).)

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.

⁹ UPR GV06 'Membership of the University'

- 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.

5 Data Management Standards

- 5.1 The University categorises and determines data access as follows:

5.1.1 'Internal'

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

(Note for guidance:

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

5.1.2 'Confidential' or 'Highly Confidential'

- i At the absolute discretion of the University, specific data may be categorised as 'Confidential' or 'Highly Confidential'.
- ii Data will be categorised as 'Confidential' or 'Highly Confidential' by the Chief Information Officer in light of recommendations from Information Asset Owner and, where appropriate, legal and other advice.

(Note for guidance:

The grounds for categorising data as 'Confidential' or 'Highly Confidential' 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'

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

5.2 Information Asset Owners

(See section 6.5, also.)

- 5.2.1 Every data source and Dataset must have a designated Information Asset Owner.
- 5.2.2 Information Asset Ownership 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 Information Asset Owner is responsible for the data quality, security and availability of the data for which they are Information Asset Owner.

5.3 Data Experts

(See section 6.6.)

Data Experts are responsible for and accountable to the relevant Information Asset Owner 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

(See section 6.7, also.)

- 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 (see section 5);
 - 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 Information Asset Owner; 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 all data and any third party use of the data must conform with Appendix II, UPR IM16¹⁰.

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

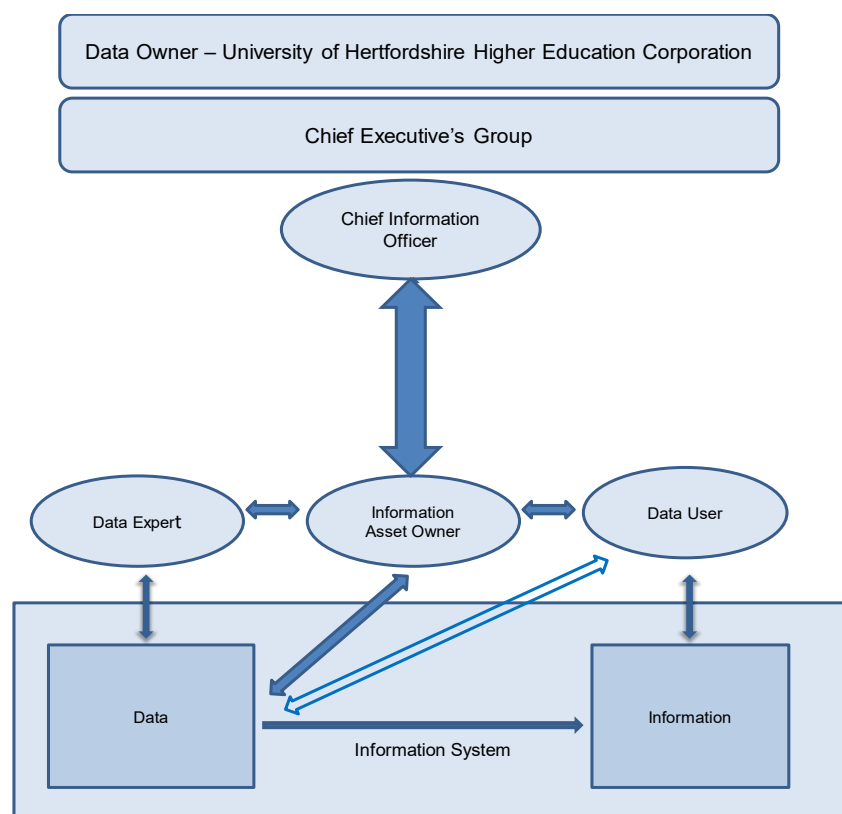
(See Appendix I, UPR IM16¹¹.)

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.

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

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

6.2 Data Management Framework



6.3 Data Owner

The University of Hertfordshire Higher Education Corporation – the Data Controller in GDPR terminology.

6.4 Chief Information Officer

6.4.1 The Chief Information Officer, advised and assisted by the Library and Computing Services Board (LCS Board), 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;
- 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 Information Asset Owners, reviewing annually, the Data Management Policy (UPR IM16).

6.5 Information Asset Owners

6.5.1 Information Asset Owners 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 Information Asset Owners 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 Information Asset Owner 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 Management Group

The Data Management Group, chaired on behalf of the Chief Information Officer by the Data Development Manager, consists of Data Experts and Library and Computing Services technical staff responsible for the University systems. It will act on behalf of the Chief Information Officer and in particular will discuss and agree:

- a University data management standards and procedures;
- b requests for data transfers and integrations between University systems;
- c data protection issues, including that approval of Data Protection Impact Assessments;
- d data integrity and security;
- e data retention criteria and archiving policies;
- f escalation of issues to the Chief Information Officer or LCS Board as appropriate.

6.8 Data Users

6.8.1 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 Information Asset Owner;
- d for obtaining permission from the Information Asset Owner 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 Information Asset Owner.

6.8.2 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 Information Asset Owner;
- 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 Information Asset Owner;
- f present the data accurately and objectively in any use that is made of it.

7 Unstructured Data

7.1 Whilst structured data is usually held within a controlled environment on University servers, unstructured data (in the form of files and documents) are usually under the control of the user who created them, and stored in file storage where access cannot be so easily centrally regulated. For this reason it is essential that the owners of those documents take responsibility for their security, dependent on the type of data which is contained within.

7.2 The University provides advice and guidance on HertsHub on where documents should be stored and how they should be protected. This guidance (which may change from time to time) must be followed in order to protect University data and personal and confidential data from accidental or deliberate leakage. In particular, data classified as 'Confidential' or 'Highly Confidential' must be protected accordingly.

7.3 The Head of the Strategic Business Unit which has responsibility for the file store in which unstructured data is held will be the Information Asset Owner where no other Information Asset Owner is defined.

8 Research Data

(See Appendix III, UPR IM16¹².)

- 8.1 Data management is an essential and integral part of the responsible conduct of research.
- 8.2 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 (see UPR RE02¹³).
- 8.3 This policy and the principles and standards that it defines also apply to the management and use of research data.

8.4 Information Asset Owner - research data

For the purposes of research data, the Principal Investigator or agreed equivalent role (such as the Principal Supervisor of Research Students) will fulfil the role and responsibilities of the Information Asset Owner 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' (see Appendix III, UPR IM16¹⁶).)

9 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 Information Asset Owners and the Data Management Group.

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.

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