## 



**Data Management and Governance Policy**

|  |  |
| --- | --- |
| **Technology & Information Strategy Forum Endorsement:** | October 2016 |
| **Management Board Endorsement:** | February 2017 |
| **Audit Committee Endorsement:** |  |
| **Board of Governors Approval:** |  |
| **Lead:** | Head of Strategy Development |
| **Date of next review:** | February 2020[1](#_bookmark6) |

1 Unless otherwise indicated this policy will still apply beyond the scheduled review date

## Introduction

The University operates in an increasingly complex, data-oriented environment which requires effective collection, management, analysis and communication of information. The data generated and held by the University are key strategic assets that must be appropriately managed to provide a solid foundation for strategic development, essential functions and academic integrity.

Ensuring appropriate governance for the management and use of data is consequently increasingly critical to the University’s operations. Inappropriate and/or ineffective governance can result in inefficiencies and exposes the University to avoidable risk. A consistent, repeatable, and sustainable approach to data governance is therefore necessary in order to protect the security and integrity of the University’s data assets.

## Policy Purpose

The primary purpose of the Policy is to establish proper standards to assure the quality and integrity of University data. The Policy also introduces a Data Management and Governance Hierarchy which provides an overview of the roles and responsibilities of University staff in relation to the management of data. Specifically, the purpose of the Data Management and Governance Policy is to:

* + Define roles and responsibilities for different levels of data usage and establish clear lines of accountability;
  + Encourage development of best practice in effective data management and protection;
  + Improve student retention and enhance the Student Experience through supporting the development of learning analytics;
  + Protect the University’s data against internal and external threats (e.g. breach of privacy and confidentiality);
  + Reinforce requirements for University staff to comply with applicable laws, regulations, and standards; and
  + Ensure that data trails are effectively documented within the processes associated with accessing, retrieving, reporting, managing and storing of data.

## Policy Scope

This policy applies to all primary sources of institutional data. This policy covers, but is not limited to, institutional data in any form, including print, electronic, audio-visual, backup and archived data.

# POLICY PRINCIPLES

The following principles outline the minimum standards that guide the University’s data governance procedures and must be adhered to by all staff:

* No one person, School or service owns institutional data, it is the property of the University and should be managed and protected as a key corporate asset;
* All data will have a single, identified Master Copy;
* Duplication of institutional data should be avoided wherever possible;
* The University will operate a data management and governance hierarchy. Through this, every identified data source must have a Data Steward who is responsible for data integrity, quality and security which will be achieved through implementation and enforcement of data management within their area of responsibility;
* Staff will be provided with training to develop and maintain those data competencies necessary to fulfil their roles and responsibilities;
* Staff will be held accountable for their use of data according to their roles and responsibilities;
* Primary source institutional data will be accessible only according to agreed needs;
* The uses of each instance of primary source data should be known, agreed and documented;
* The value and utility of institutional data will be enhanced through metadata which will be recorded and managed in a data dictionary;
* The University will use and retain personally identifiable information only for the purposes agreed when it was collected. Personal use of institutional data is prohibited;
* Data shall be retained and disposed of in an appropriate manner in accordance with the University’s Records Management Policy and its retention schedules;
* The University will, at all times, operate in accordance with the Data Protection Act.

# DATA MANAGEMENT AND GOVERNANCE HIERARCHY

This section outlines the access rights, roles and responsibilities of University staff in relation to the management and protection of data. The successful prosecution of formal data governance is dependent upon ensuring that employees are held accountable for their management of data. The University achieves this through the following clearly-defined data roles:

## Data Owner

Cardiff Metropolitan University.

## Data Trustee

Typically a Level-3 manager with responsibility for a business function, Data Trustees are accountable for managing, protecting and ensuring the integrity and usefulness of the University data held within their departments. Data Trustees are responsible for:

* establishing standards and procedures for the management of data;
* ensuring implementation of and compliance with data management policy, standards and procedures;
* adjudicating on data-related disputes that may arise.

## Data Steward

Typically a Level-4 manager the Data Steward will have delegated decision-making authority for data management. Data Stewards may represent Data Trustees in policy discussions, architecture discussions and/or in decision-making forums. Data Stewards actively participate in the establishment and prosecution of data management processes. It is necessary that Data Stewards understand the business requirements of the University’s functions and are able to facilitate access to data. In the event that a Data Steward has questions about the legitimacy of a specified business need, the Data Steward will validate the request with the appropriate Data Trustee. Data Stewards are responsible and accountable to Data Trustees for:

* the management of assigned institutional data;
* establishment and maintenance of a data dictionary;
* co-ordination of associated Data Experts;
* providing advice to the Data Governance Committee on data management issues, policy and procedures;
* data quality;
* promotion of University data as a key strategic corporate asset;
* authorisation of third-party access to assigned institutional data;
* facilitation of data-sharing and integration;
* liaising with other Data Stewards;

## Data Expert

Data Experts are University employees who work with institutional data on a daily-basis in order to perform assigned duties or functions. Database administrators and employees engaged in the development of management information and business intelligence fall into this category. Data Experts are responsible and accountable to Data Stewards for:

* the operational management and integrity of the data assigned to them;
* applying University data management standards and procedures;
* effective liaison with Data Stewards and Custodians;
* data analysis;
* providing information to support University decision-making;
* external reporting requirements;
* resolving data queries;
* implementation of the University Records Management Policy and associated retention schedules;
* generating meta-data and contributing to a user-friendly data dictionary

## Data Custodian

Generally located in Information Services, Data Custodians are systems administrators responsible for the operation and management of systems and servers which collect, manage and provide access to institutional data. Data Custodians may not extend the use of University data beyond the initial scope without additional review by the appropriate Data Steward.

## Data User

Data Users are University employees who have been granted access to institutional data in order to perform assigned duties or functions. Data Users are responsible and accountable to their managers for:

* complying with the defined data policy and data management standards and procedures;
* the use and distribution of data accessed from corporate systems;
* identifying and seeking advice upon any potential conflict of interest resulting from data access granted to them;
* for contributing to the accuracy and integrity of data through providing timely notification of errors to the relevant Data Steward;
* not disclosing data to unauthorised persons without the consent of the relevant Data Steward.

# RESEARCH DATA MANAGEMENT

Data management is an essential component in the responsible and sustainable conduct of research. The University is responsible for:

* 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;
* 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;
* for supporting investigation into any allegations of misconduct or regulatory breach.

# POLICY IMPLEMENTATION AND REVIEW

Implementation of the Policy will be overseen by the Data Governance Committee which is chaired by the Head of Strategy Development and reports to the Technology and Information Strategy Forum. Membership of the Committee consists of Data Trustees, Stewards, Custodians, Experts and Users. The Committee is responsible for monitoring and reviewing the effectiveness of data management policy, standards and procedures.

This Policy will be reviewed and updated every three years from the approval date, or more frequently if appropriate. In this regard, any staff members who wish to make any comments about the Policy may forward their suggestions to the Head of Strategy Development.

# GLOSSARY OF TERMS

To establish operational definitions and facilitate ease of reference, the following terms are defined:

**Data** – distinct units of information such as numbers, letters or symbols, usually formatted in a specific way, stored in a database and suitable for processing by a computer.

**Data Quality** – the accuracy, completeness, validity and currency of the data;

**Information** – data combined and processed into a meaningful form via an information system;

**Access** – the right to read, copy, or query data.

**Institutional Data** – University information resources and administrative records created, acquired or maintained by University employees in performance of their duties. These data can generally be assigned to one of four categories:

* Public access data – data that is openly available to all staff, students, and the general public;
* Internal general data – data used for University administration activities and not for external distribution unless otherwise authorised;
* Internal protected data – data that is only available to staff with the required access in order to perform their assigned duties; and
* Internal restricted data – data that is of a sensitive or confidential nature and is restricted from general distribution. Special authorisation must be approved before access or limited access is granted.

***Metadata*** – can be defined as structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use or manage an information source. A common shorthand description refers to metadata as ‘data about data’. The foundation of a data dictionary.

***Data Security*** – refers to the protection of University data in relation to the following criteria:

* Access control;
* Authentication;
* Effective incident detection, reporting and solution;
* Physical and virtual security; and
* Change management and version control.

# APPENDIX 2

**Proposed Schedule of Data Governance Committee Business**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | 2017 | | 2018 | | 2019 | |
| Winter | Summer | Winter | Summer | Winter | Summer |
| Agree and communicate a Data Management and  Governance Policy |  |  |  |  |  |  |
| Undertake an audit of Data Systems and Owners to assist in identifying and releasing valuable corporate data and in  assigning data roles |  |  |  |  |  |  |
| Support owners of data systems in the publication of useful, high-quality management information (MI) and business intelligence (BI) |  |  |  |  |  |  |
| Review use of metadata across University data sources and make recommendations for implementing a  standardised approach |  |  |  |  |  |  |
| Development of a register of ‘Data Roles’ and updating of  JDs/Contracts as necessary |  |  |  |  |  |  |
| Develop and consult upon a standardised ‘Data Access’ process |  |  |  |  |  |  |
| Establish a Learning Analytics Sub-Group |  |  |  |  |  |  |
| Develop and consult upon a Learning Analytics Policy |  |  |  |  |  |  |
| Participate in Jisc Learning Analytics Pilot Project |  |  |  |  |  |  |
| Evaluate potential benefits of establishing a data warehouse and, if appropriate, make a business case for investment |  |  |  |  |  |  |
| DGC Annual Review of Progress |  |  |  |  |  |  |
| LA Sub-Group Annual Review of Progress |  |  |  |  |  |  |