Academic Board

COVER SHEET

|  |  |  |
| --- | --- | --- |
| 06-03-2024 | 09:00 | Via MS Teams |

**Key Details**

|  |  |
| --- | --- |
| Title of report | Data Management and Governance Policy |
| Date of report | 27 February 2024 |
| Author(s) & e-mail address | Mairwen Harris ([mharris3@cardiffmet.ac.uk](mailto:mharris3@cardiffmet.ac.uk))  Mohamed Maher ([mmaher@cardiffmet.ac.uk](mailto:mmaher@cardiffmet.ac.uk)) |
| Department | Strategy, Planning and Performance |
| UEG Sponsor | University Secretary |
| Executive Summary | This is an update of the Data Management and Governance Policy. The policy has been endorsed by the Data Super Users Group and comments sought from the Director of Digital and Libraries. |
| Recommendations |  |
| Action required | Approve |
| Document Type | Open |
| Index number | AB14.1/06.03.24 |

**Implications of Report**

|  |  |
| --- | --- |
| Financial | Ensuring appropriate governance for the management and use of its data are critical to the University’s operations. |
| Risk | Inappropriate and/or ineffective governance can result in inefficiencies and exposes the University to avoidable risk. |
| EDI | Upholding robust data governance is essential in relation to protecting EDI data. |
| Strategy | Ensuring appropriate governance for the management and use of its data are critical to the University’s operations and will enable data informed decision making crucial to monitor KPIs and help deliver the strategy. |
| Other | N/A |

# Approval Route

|  |  |
| --- | --- |
| 12-02-2024 | Data Super Users Group [endorsed] |
| 06-03-2024 | Academic Board [for approval] |

Length of Paper: 8 pages (including coversheet)



**Data Management and Governance Policy**

|  |  |
| --- | --- |
| **Academic Board Approval:** | March 2024 |
| **Lead:** | Head of Strategy, Planning and Performance |
| **Date of next review:** | March 2027 |

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

# Introduction

The University operates in an increasingly complex, data-oriented environment requiring effective collection, management, analysis and information communication. 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 its data are critical to the University’s operations. Inappropriate and/or ineffective governance can result in inefficiencies and exposes the University to avoidable risk. Therefore, a consistent, repeatable, and sustainable approach to data governance is necessary to protect the security and integrity of the University’s data assets.

# Policy Purpose

The primary purpose of this 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 which:

* + 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;
  + Ensure that data trails are effectively documented within the processes associated with accessing, retrieving, reporting, managing and storing of data; and
  + Enhance research and innovation.

This policy emphasises data's pivotal role in academic progress, upholding robust data governance empowers researchers and maintains our leadership in pioneering scholarship.

# 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.

This policy intends to be consistent with relevant University policies (such as Data Protection Policy, Freedom of Information Policy, Information Security Policy, Records Management Policy and IT Acceptable Use Policy) and all applicable legal and regulatory compliance requirements including, but not limited to, Principle 7 of the Data Protection Act (1998), the Accountability and Governance aspects of the General Data Protection Regulations (2016) and Freedom of Information Act (2000).

# Data management

* + **Data governance:** The Data Super Users Group will establish a data governance framework to manage and oversee data-related activities. This framework will include policies, procedures, roles, and responsibilities to ensure the integrity, availability, and security of the University's data assets.
  + **Data quality:** The University is committed to ensuring that data is accurate, complete, and consistent. Data quality standards will be established and monitored to ensure that data meets the needs of its intended users.
  + **Data privacy and security:** The University is committed to protecting the privacy and security of personal and sensitive data. Appropriate security measures will be implemented to safeguard data against unauthorised access, theft, loss, or misuse.
  + **Data retention and disposal:** The Data Super Users Group will work with the Compliance team to establish policies and procedures for the retention and disposal of data. These policies will ensure that data is retained for as long as required by law or regulation and that it is disposed of securely and appropriately.
  + **Data access and sharing:** The Data Super Users Group will establish policies and procedures for granting access to data and sharing data with external parties. Access will be granted based on the principle of least privilege, and data will only be shared with external parties in accordance with legal and regulatory requirements.
  + **Data literacy and training:** All data users will receive appropriate training and support to ensure that they understand their roles and responsibilities in relation to data management.

# 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:

A set of data policy principles have been drafted to provide a foundation for our data governance framework. These principles outline the minimum standards for data ownership, management, privacy, and security that all staff are required to adhere to. The principles are designed to create a culture of responsible data use that supports evidence-based decision-making, fosters innovation, and upholds the highest standards of ethical and legal conduct.

1. **Ownership of institutional data:** 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.
2. **Single Master copy:** All data will have a single, identified Master Copy to ensure consistency and reduce the risk of data discrepancies.
3. **Avoidance of data duplication:** Duplication of institutional data should be avoided wherever possible to reduce the risk of errors, inconsistencies and unnecessary storage costs.
4. **Data management and governance hierarchy:** The University will operate a data management and governance hierarchy. Every identified data source must have a Data Steward who is responsible for data integrity, quality and security, which will be achieved through the implementation and enforcement of data management within their area of responsibility.
5. **Training and competencies:** Staff will be provided with training to develop and maintain those data competencies necessary to fulfil their roles and responsibilities.
6. **Accountability:** Staff will be held accountable for their use of data according to their roles and responsibilities.
7. **Access to primary source institutional data:** Primary source institutional data will be accessible only according to agreed needs.
8. **Documentation of data uses:** The uses of each instance of primary source data should be known, agreed and documented.
9. **Metadata and data dictionary:** The value and utility of institutional data will be enhanced through metadata which will be recorded and managed in a data dictionary. A high-level data dictionary will be maintained for all University datasets available as a central report which will provide a consistent definition for every field.
10. **Data privacy and confidentiality:** The University will use and retain personally identifiable information only for the purposes agreed upon and these will be state in the data definition articulating when it was collected. Personal use of institutional data is prohibited.
11. **Data retention and disposal:** Data shall be retained and disposed of appropriately in accordance with the University’s Records Management Policy and its retention schedules.
12. **Compliance with statutory requirements:** The University will, at all times, operate in compliance with all applicable data protection and privacy laws, regulations, and guidelines, including but not limited to the Data Protection Act, the General Data Protection Regulation (GDPR), and any other relevant statutory requirements.

# 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 Super Users Group**

* + The data Super Users Group will oversee the data governance policy and related procedures. It will ensure that the policy and procedures are followed, updated, reviewed and approved, whilst providing guidance and support to stakeholders.
  + The group will review and address data-related issues and challenges in conjunction with relevant committees and groups to prioritise data management projects and initiatives. It will serve as a resource for University committees/groups and departments on data-related issues and challenges.

**Data Super Users**

* + Data super users will be members of the Data Super Users Group and act as advocates for data integrity, governance, and best practices in their respective areas of responsibility.
  + They will provide guidance and support to other users in their respective areas of responsibility, including identifying and addressing data management challenges and opportunities. Ensure consistency and accuracy of data definitions, policies, and procedures within their respective areas of responsibility.
  + As part of the Data Super Users Group they will act as a bridge between IT and business users, providing feedback on data management processes and systems. They will identify opportunities for improving data management, including data quality, accessibility, and visibility.

**Data Stewards**

* + Data stewards are responsible for managing specific data domains. They ensure that the data is accurate, consistent, and adequately documented. They work closely with data owners and users to establish and maintain data standards and definitions. They are responsible for identifying and addressing data quality issues, managing data access permissions, and ensuring data are used responsibly and ethically.
  + Data stewards will define and maintain data definitions, policies, and procedures for their respective areas of responsibility. Identify and address data management challenges and opportunities within their respective areas of responsibility. Any conflicts or issues will be taken to the Data Super Users Group for advice and guidance.
  + Data stewards will be appointed for each data domain to ensure that data is managed in accordance with established policies and procedures. Data stewards will be responsible for monitoring data quality, managing access to data, and ensuring that data is used in a responsible and ethical manner.

**Data Custodians**

* + Data custodians are responsible for the day-to-day management of specific data sets. They ensure that the data is properly stored, secured, and backed up. They also ensure that the data is available to authorised users when needed. They work closely with data stewards to ensure that data is correctly classified and that access to sensitive data is restricted to authorised users.

**Data Owners**

* + Data owners are responsible for the overall management and governance of specific data sets. They are responsible for defining data standards and definitions and ensuring that data is properly classified and protected. They work closely with data stewards and custodians to ensure that data is appropriately managed throughout its lifecycle.
  + Data owners are responsible for the accuracy, completeness, and timeliness of the data under their control. They must ensure that access to the data is appropriate and that the data is stored, processed, and transmitted securely.

**Data Users**

* + Data users are responsible for using data in a responsible and ethical manner. They are responsible for ensuring that the data they use is accurate, consistent, and properly documented. They work closely with data stewards to ensure that data standards and definitions are articulated, understood and followed.

# 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 Super Users Group which is chaired by the Head of Strategy, Planning and Performance and reports to the Academic Board. Membership of the group consists of Data Stewards, Custodians, Owners and Users. The group 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 planning and Performance.

# 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.

**Data domain** - a specific area or subject matter within Cardiff Met’s data landscape characterised by a common theme, purpose, or function. Data domains help categorise and organise data for effective management and analysis.

**Data sets** - collections of related data elements or objects that are grouped together for a specific purpose, often in a tabular format. Data sets can include various data types, such as numerical, textual, or categorical, and are used for analysis, reporting, and decision-making.

**Primary data source** - the original or authoritative location from which data is obtained or generated within the university. This source provides the most reliable and unaltered data version and serves as the foundation for data analysis and decision-making processes.

APPENDIX 1

**Terms of Reference: Data Super Users Group**

# Purpose:

The Data Super Users Group will provide a forum for data professionals from across the University who are experts in data management to offer guidance and support to other users, identify and disseminate best practice.

# Core business:

The data super user group will play an essential role in the data integrity project by providing a forum for data professionals, ensuring that data management is handled effectively and efficiently and that the expertise of individuals who are already working with data is utilised.

# The group will:

* Provide guidance and support to other users on data management processes and systems.
* Review existing reports and data systems with a view to create consistency across the institution.
* Establish best practices for creating new reports.
* Establish robust data governance and compliance procedures for the institution.
* Review data definitions for reporting.
* Identify and address data management challenges and opportunities.
* Ensure data consistency and accuracy by promoting a culture of data reliability and accuracy.
* Provide feedback on data management processes and systems and to act as a bridge between IT and business.
* Promote a culture of data openness, sharing, transparency and visibility.
* Ensure data visibility and access to all relevant stakeholders.
* Ensure data security and compliance with data privacy regulations.
* Enhance data management technology and infrastructure by reviewing systems and leveraging new technologies as appropriate.
* Provide training and development opportunities for the workforce to improve data management, data literacy, skills and knowledge.