

Table of Contents

1. Purpose
2. Scope
3. Responsibilities for Data Quality and Data Quality Assurance
 - Audit and Scrutiny Committee
 - Data Assurance Group
 - Data Stewardship
 - Institutional Responsibility
4. Risk Associated with Data
5. Quality Data Characteristics
6. Data Quality Objectives
 - Appropriate Responsibility, Accountability, and Awareness
 - Appropriate Policies and Procedures
 - Appropriate Systems and Processes
 - Appropriate Security
 - Appropriate Staff Development
7. Reporting and Representation of Data
8. Implementing this Policy
9. Remit of Data Governance Groups
 - Data Governance Group (DGG)
 - Data Executive Group (DEG)
 - Data Assurance Group (DAG)

Data Quality and Data Quality Assurance Policy

Purpose

1. The University needs timely, accurate and reliable data in order to manage activities and meet internal and external requirements to demonstrate accountability through accurate reporting.
2. Specifically, the University needs to ensure its data quality so that it can:
 - Provide effective and efficient services to students, staff and other stakeholders.
 - Produce accurate and comprehensive management information on which timely, informed decisions can be made to inform the future of the institution.
 - Monitor and review activities and operations.
 - Produce accurate external returns to ensure accurate funding allocations, and to demonstrate accountability to public and private funders.
 - Meet the terms of the Model Financial Memorandum between HEFCE (and its successor bodies) and institutions.

Scope

3. The scope of this policy includes data held in the institution on all University-wide systems, and any data collected from these systems that are used to inform analysis and reporting.
4. This policy will inform an annual process of assuring data quality overseen by the Data Assurance Group, and reported to the Audit and Scrutiny Committee, and will fit within a framework of information to support the aims and objectives of data assurance, and related policies for the University.

Responsibility for Data Quality and Data Quality Assurance

Audit and Scrutiny Committee

5. The HEFCE Financial Memorandum and Accountability and Audit Code of Practice, August 2008, introduced a new requirement for the Audit and Scrutiny Committee to give, as part of their annual opinion, assurance over management and quality assurance of data submitted to HESA and to HEFCE and other funding bodies. The Code states:

"...we are seeking assurances from designated officers and audit committees about the management and quality assurance arrangements for data submitted to the Higher Education Statistics Agency (HESA), HEFCE and other funding bodies. This is imperative in order to improve the reliability of data which is crucial for the efficiency of our funding and to reduce the number of significant funding adjustments needed to correct data errors. We endorse guidance on the principles of data management for public bodies as published in November 2007 by the Audit Commission, 'Improving information to support decision making: standards for better quality data'." (Para. 6, page 9)

HEFCE's guidance to audit committees on how they need to reach the required opinion on data quality states that the committee 'needs to be sure that management has assessed the risks posed by data accuracy and taken appropriate mitigating actions'.

Institutional responsibility

6. Although ultimate responsibility for data quality assurance lies with Council, it is an integral part of the role of all members of staff to ensure that they follow the principles of this policy in order to maximise the accuracy, timeliness and quality of data collected and recorded, analysed and reported.

Risk Associated with Data

7. Key risks relating to data are as follows:
 - Mandatory conditions of grant could be breached.
 - Data could give misleading external and internal impressions of institutional performance in teaching and research.
 - Poor data could result in inappropriate decision-making across the institution.
 - Poor data could result in reputational damage in areas such as student recruitment and access, and student records.
 - Poor data could lead to inadequate reporting to sponsors of research, resulting in financial penalties from funders or, depending upon the extent of the problem, reputational damage and diminished funding for research.
 - Inaccurate data could lead to under-funding.
 - Inaccurate data could lead to over-funding with subsequent claw-back of overpaid funds which, if significant, could impact adversely on the institution's financial health.
 - Inaccurate data could lead to reduced future funding (holdback) thereby undermining the cash flow forecasts and adversely affecting financial health.
 - [The University includes failure to ensure appropriate data quality on its risk register.]

Quality Data Characteristics

8. In March 2007, the Audit Commission published a framework to support improvement in data quality in the public sector. This framework includes six key characteristics of good quality data, to which the University has added one further characteristic, and which may be summarised as follows:

- a. **Accuracy**

- Data should provide a clear representation of the activity/interaction
- Data should be in sufficient detail
- Data should be captured once only as close to the point of activity as possible

- b. **Validity**

- Data should be recorded and used in accordance with agreed requirements, rules and definitions to ensure integrity and consistency
- c. **Reliability**
- Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflects any changes in performance
- d. **Timeliness**
- Data should be collected and recorded as quickly as possible after the event or activity
 - Data should remain available for the intended use within a reasonable or agreed time period
- e. **Relevance**
- Data should be relevant for the purposes for which it is used
 - Data requirements should be clearly specified and regularly reviewed to reflect any change in needs
 - The amount of data collected should be proportionate to the value gained from it
- f. **Completeness**
- Data should be complete
 - Data should not contain redundant records
- g. **Compliance**
- Data must comply with regulations on data protection and data security

Data Quality Objectives

9. The characteristics of good quality in the points above provide the criteria against which the significance and purpose of the data must be balanced. The objectives are set out below and the bullet points indicate the approach to achieving them.
- a. **Appropriate Responsibility, Accountability and Awareness**
- Every member of staff should recognise the need for good quality data and how they can contribute to it
 - Every member of staff should be aware of their individual responsibilities with regard to data collection, storage, analysis and reporting
 - Every member of staff should be aware of the implications of poor data quality in their area in terms of internal and external accountability including those affecting other departments and the institution as a whole
 - Every member of staff should report any systematic data quality issues immediately to their manager who should ensure remedial action is taken
 - Every member of staff should be aware of the policies related to data quality on security and data protection
- b. **Appropriate Policies and Procedures**
- The institution should define clearly its key data requirements and assurance arrangements
 - Local procedures must exist for all key activities such as major data collection exercises and external returns
 - All such policies and procedures should be reviewed regularly to consider their impact on data quality and to ensure they reflect any change in need

- Departmental managers should ensure that all such policies and procedures are adopted and embedded within working processes and that compliance is achieved
- c. Appropriate Systems and Processes
- Clear systems and business processes should exist in which data collection and reporting are an integral part
 - Guidelines for all processes supporting key data requirements as defined by the institution should exist and be followed consistently across the institution
 - Data should be collected and recorded once only wherever possible without the need for multiple systems
 - Data collection systems should contain internal validation to ensure accurate and complete data
 - University-wide systems should have internal validation checking facilities to ensure data is complete, consistent and internally validated
 - All systems should be electronic wherever possible to reduce the risk of manual error, except where there is a need to collect, process and store original documents
 - There should be clear strategies for data storage and archiving from systems, with retrieval and security appropriate to an evaluation of present value and future use
- d. Appropriate Security
- The institution should have in place appropriate security arrangements to ensure that data is protected from unauthorised access from outside the institution
 - All University-wide systems should have security arrangements in place to ensure appropriate levels of access to data by individual staff and students
- e. Appropriate Staff Development
- All members of staff accessing, inputting and amending data on University-wide systems should have the appropriate knowledge, competencies and capacity to carry out the activity and preserve data quality
 - All policies procedures and guidelines should be communicated effectively to relevant staff, and this will include policies on security and data protection as part of the wider consideration of data quality
 - Appropriate staff development should be provided at induction and periodically to enable staff to meet the objectives of this policy, and be reviewed at PDR and updated to reflect any change in need
 - Responsibility for data quality should be included in job descriptions with significant data handling or management responsibilities

Reporting and Representation of Data

12. All management information reports should be clear in what they are representing, bearing in mind the audience for which they are intended, and regular reports should be reviewed to ensure that they reflect any change in need. The review should be balanced with the need for consistency over time so that trends can be recognised and reported.
13. External returns should be subject to rigorous validation and verification, submitted on a timely basis and should evidence a full audit trail, including appropriate approval and sign-off as specified by the body to whom the return is submitted, or agreed by the Data Assurance Group in the absence of such a recommendation. The person producing the return should not be responsible for the final sign-off which should be completed by a senior manager, if not by a senior officer.

Implementing this Policy

14. This policy will be communicated to all those involved in data quality and will be prominently displayed on the University web-site. It is the responsibility of senior managers to ensure that staff who are working with data are aware of the policy and understand how it relates to their work.
15. The policy will be the overarching policy for the University but will fit within the framework of documentation appropriate to the different areas of responsibility for data.

Remit of Data Groups

16. The Remit of the Data Governance Group (DGG) is as follows:
 - a. Communicate, maintain, and encourage a culture that values data quality throughout the University, promoting data governance as a key enabler for this.
 - b. Promote engagement with the Data Strategy, Data Quality Policy and data governance, leading cross-domain collaboration to resolve data issues and deliver improvements in line with the agreed roadmap
 - c. Monitor the effectiveness of the Data Strategy implementation; the Data Quality Policy and the Data Operating Model, identifying risks and issues and recommending remedial action as appropriate
17. The remit of the Data Executive group (DEG) is as follows:
 - a. Take ownership of, and ensure the effectiveness of, the University's Data Strategy, Data Quality Policy and their implementation
 - b. Manage and resolve risks/policy gaps where remediation is necessary
 - c. Support the development of an ongoing data governance function, including empowering and supporting a network of Data Executives, Stewards, Producers, and Consumers, to contribute to data governance, and improvement and maintenance of data quality as appropriate
18. The remit of the Data Assurance Group is as follows:
 - a. The Data Assurance Group (DAG) will be responsible to the Audit and Scrutiny Committee (ASC) for oversight of a University framework for management and accountability of data quality.
 - b. DAG will report to ASC as required, but at least on an annual basis.
 - c. The Chair of DAG will be appointed by the Registrar and will be a senior individual at top management level with strategic responsibility for the management and co-ordination of data quality assurance, noting that operational issues are the responsibility of the senior managers and teams responsible for congruent areas.
 - d. Members of DAG will include, but will not be limited to, the senior managers responsible for data and for major external data returns for the University. There will also be a senior member of IT Services with responsibility for systems from which the data is drawn. The DAG will ensure that data assurance policies which cover congruent

groupings, are in place and are kept up to date. Each area will have a nominated senior individual responsible for data quality:

- Finance Data
 - Student Data
 - Staff Data
 - Estates Data
 - Research Data
- e. The Group will liaise with those responsible for risk, assurance, data protection and data security at the University level.
- f. DAG will consider the wider strategic and policy issues relating to the need to give assurance to the Audit and Scrutiny Committee, including work with internal and external audit.
- g. DAG will have standing items on a termly agenda which ensure review and revision of data assurance issues, to ensure that material changes are co-ordinated and communicated.

Revisions drafted: 02/10/2024

Reviewed by Data Governance Group: 05/12/2024

Reviewed by Data Governance Group: 26/11/2024