Data Quality Policy

Contents

Overview and Purpose 2

Scope 2

Policy 3

- Governance and Leadership 3
- Policies and Plans 4
- Systems and Processes 4
- People and Skills 5
- Data use and reporting 6

Related Legislation, Regulations and Policies 7

Breach of Policy 7

OVERVIEW AND PURPOSE

1. Kingston University recognises the value of the data that we process and is committed to maintaining high standards in its management of data.

2. The University recognises its responsibilities for quality of personal data under legislation including the General Data Protection Regulation (GDPR), Data Protection Act (DPA) 2018 and the Privacy and Electronic Communications Regulations (PECR), together with the requirements of the Office for Students (OfS), via their partners including the Higher Education Statistics Agency (HESA).

3. The University requires good quality data to:

   - Meet its obligations under Data Protection legislation
   - Produce accurate statutory returns, thereby securing appropriate and fully justified funding allocations and provide accurate representations of institutional performance
   - Provide accurate data to meet its obligations under equalities, freedom of information and safety legislation
   - Produce appropriate and accurate management information to inform institutional planning and decision-making
   - Deliver efficient services to students, staff and other stakeholders.

4. Article 5 of the GDPR includes the following data quality principles relating to processing of personal data:

   1. Personal data shall be:

   …
   c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
   d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy); …
   e) kept in a form which permits identification of data subjects for no longer than is necessary … ('storage limitation'); …

SCOPE

5. This policy applies to all staff, students and affiliates.

6. This policy covers all data processed by the University for the purposes of managing its activities, whether on corporate information systems or in manual form. It does not cover data held by the University where the data owner is a third party, such as

student coursework, nor does it cover research data for which the institution may nonetheless own the intellectual property rights. Policies regarding good research practice and intellectual property rights can be viewed on the University website.

POLICY

GOVERNANCE AND LEADERSHIP

7. There is clear corporate leadership of data quality by those charged with governance.
8. The Vice Chancellor is the Accountable Officer and has overall responsibility for the quality of data provided to Designated Data Bodies (DDBs). Responsibility to ensure effective arrangements are in place to facilitate the submission of appropriate and accurate data returns to external stakeholders and regulatory bodies has been delegated to the University Secretary.
9. The University Secretary is the University Senior Leadership Team member with overall responsibility for data assurance. The University Secretary will attend, as a minimum, the appropriate IGC meeting where the annual data quality assurance report is presented for discussion.
10. A senior individual at top management level (for example a member of the senior leadership team) has strategic responsibility for data quality for their area, and this responsibility is not delegated.
11. The corporate objectives for data quality are clearly defined and have been agreed at Senior Leadership Team level.
12. The data quality objectives are linked to business objectives, cover all the university's activities, and have an associated delivery plan.
13. The commitment to data quality is communicated clearly, reinforcing the message that all staff have a responsibility for data quality.
14. Accountability for data quality is clearly defined and is considered where relevant as part of the performance appraisal system.
15. There is a framework in place to monitor and review data quality, with robust scrutiny by those charged with governance. The programme is proportionate to risk.
16. Data quality is embedded in risk management arrangements, with regular assessment of the risks associated with unreliable or inaccurate data.
17. Where applicable, the university has taken action to address the results of previous internal and external reviews of data quality.
18. Where there is joint working, there is an agreement covering data quality with partners (for example, in the form of a data sharing protocol, statement, or service level agreement).

19. The Data Quality Assurance Group (a sub-group of the Information Governance Committee) provides assurance to the Information Governance Committee, who then assure the University Secretary, SLT and board on the quality of all statutory returns data.

Policies and Plans

20. The University's arrangements for the management and quality assurance of data are clearly defined at an institutional level in this Data Quality Policy. The Data Quality Policy is reviewed regularly, and at least annually, by the Information Governance Committee.

21. Returns to the OfS and other statutory returns are classified by the Data Quality Assurance Group as high, medium or low risk, depending on funding impact, league table impact and complexity, whether it is already scrutinised by another committee or team, or audited internally or externally.

22. Data Quality Plans are in place for OfS and other statutory returns, detailing data quality control methods.

23. Plans are reviewed regularly, and at least annually, by the Data Quality Assurance Group and updated for any changes in requirements.

24. The Policy and Plans are fully adopted and complied with in the context of working practices.

25. Data Quality Assurance reports are optionally completed for high-risk statutory returns on an annual basis and reviewed by the Data Quality Assurance Group.

26. Significant risks and actions from Data Quality Plans and Assurance reports are documented in the Data Quality Risk Register and escalated from the Data Quality Assurance Group to the Information Governance Committee.

27. A summary of data quality assurance is provided to ARAC on an annual basis by the Information Governance Committee.

Systems and Processes

28. Systems and processes are in place for the collection, recording, analysis and reporting of data, which are focused on securing data which are accurate, valid, reliable, timely, relevant and complete.

29. Systems and processes work according to the principle of right first time, rather than employing extensive data correction, cleansing or manipulation processes to produce the information required, where possible.

30. Arrangements for processing data are integrated into the business planning and management processes of the University, supporting the day-to-day work of staff.

31. The need for data should be periodically reviewed to ensure it is necessary and processed by the most secure and efficient means possible.

32. Data should be scrutinised on a regular basis for reasonableness, accuracy and fitness for purpose to identify and address errors or missing values.

33. Information systems are appropriately integrated wherever possible to minimise unnecessary duplication of data processing. Data should be entered once and in the formally agreed system of record (golden source), then disseminated to other systems in close to real time.

34. Information systems have in-built controls that prevent erroneous data entry, and which verify the consistency and completeness of data.

People and Skills

35. Specific roles and responsibilities in relation to data quality are clearly defined and understood by the relevant individuals.

Role	Description
Data trustee	Accountable for the strategic co-ordination of data management and reporting. Is the senior risk owner, accountable for information risks. Usually a member of SLT.
Data custodian	Accountable for data processing within a defined area; oversees the capture, maintenance and dissemination of information. Is the risk owner, responsible for managing and resolving information risks. Usually the head of a function. Responsible for determining and establishing data quality controls and standards. Responsible for training, monitoring and managing data stewards and administrators. May also be the owner of OfS and statutory returns, responsible for timely and accurate completion, reporting to the Data Quality Assurance Group, and identifying new returns.
Data steward	Responsible for monitoring adherence to data quality controls and standards. May identify and resolve information risks on behalf of the risk owner. May have delegated responsibilities from Data Custodian. May be the head of a team or a management information specialist within a function. This role may be merged with Data Custodian or Data Administrator in smaller teams.
Data administrator	Responsible for capturing, recording and sharing data to quality standards. Responsible for understanding the purpose and context of the processes they operate. May identify information risks to the risk owner.
Data user	Any member of staff who uses data in their work – effectively all staff. Responsible for understanding their data duties and for completing compliance training. May identify information risks to the risk owner.
Data champion	A local point of contact for queries relating to data quality and data protection. Disseminating knowledge and awareness within their teams. Supporting risk owners to resolve risks.

Data subject	The person to whom data relates, including staff, students, affiliates, and research subjects. Responsible for providing and updating their own personal data.

36. In smaller teams, one person may hold more than one role.
37. Data users (all staff) are aware of their personal statutory responsibilities under Data Protection legislation.
38. Data users (all staff) recognise the internal and external requirements for University data to be of good quality and understand how they can contribute towards achieving this aim.
39. Data users (all staff) are aware of relevant local procedures for reporting any concerns regarding systemic data quality issues.
40. Data quality responsibilities are incorporated into job descriptions where appropriate.
41. Data quality standards are set, and staff are assessed against these.
42. There are no single points of dependency; knowledge of procedures for statutory returns is documented and shared.
43. Appropriate role-specific development and training will be provided to equip staff with the necessary skills to meet these objectives

DATA USE AND REPORTING

44. Internal and external reporting requirements have been critically assessed. Data provision is reviewed regularly to ensure it is aligned to these needs.
45. Data used for reporting to those charged with governance are also used for day-to-day management of the body's business. As a minimum, reported data, and the way they are used, are fed back to those who create them to reinforce understanding of their wider role and importance.
46. Data are used appropriately to support the levels of reporting and decision making needed. Management action is taken to address service delivery issues identified by reporting.
47. Data used for external reporting are subject to rigorous verification, and to senior management approval.
48. All data returns are prepared and submitted on a timely basis and are supported by a clear and complete audit trail.
49. Data in the return used in league tables is reviewed for accuracy and the potential impact on the university's league table position has been understood.

RELATED LEGISLATION, REGULATIONS AND POLICIES

50. This policy should be read in conjunction with other relevant University policies and documents which can be viewed in the Information regulations section of the University website.

BREACH OF POLICY

51. Anybody handling personal data agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be subject to warnings, verbal and written. In serious cases individuals will be subject to the University's disciplinary procedures, and possible legal action.