Data Quality Policy

Purpose

1.1 High quality data is essential to the production of robust institutional management information, which both enables decision making and informs planning. The university needs timely, accurate and reliable data to enable compliance with internal and external requirements to demonstrate accountability.

1.2 Imperial is committed to the achieving the highest standards of data quality and it is the responsibility of every member of staff to check that all data within their area of responsibility is accurate, accessible and complete as far as is reasonably practical.

1.3 This Data Quality Policy ("the Policy") aims to provide an overall framework so that high quality data is submitted by the university to external bodies.

1.4 The university measures the quality of its data against the following key characteristics:

- Accuracy

  Data should be sufficiently accurate for its intended purposes. Accuracy is most likely to be secured if data are captured as close to the point of activity as possible. Data should be captured once only, although they may have multiple uses. The importance of the uses for the data must be balanced with the costs and effort of collection. Where compromises have to be made on accuracy, the resulting limitations of the data should be clear.

- Validity

  Data should be recorded in compliance with relevant requirements, including the correct application of any rules or definitions. Where proxy data are used to compensate for an absence of actual data, organisations must consider how well these data are able to satisfy the intended purpose.

- Reliability

  Data should reflect stable and consistent data collection processes across collection points and over time. Users of the data should be confident that improvements reflect real changes rather than variations in data collection approaches or methods.

- Timeliness

  Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period.

- Relevance

Data captured should be relevant to the purposes for which they are used. This entails periodic reviews of requirements to reflect changing needs.

- Completeness

Data requirements should be clearly specified based on the information needs of the body and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

In addition to the characteristics outlined above, the HESA Code of Practice for Higher Education data collections[1] identifies three principles for data preparations that should inform the actions of any data owners and handlers across the university.

- Honesty

Data should genuinely reflect the characteristics, events, and objects being reported on, to the best of the university's ability. Processes and systems to collect, prepare, and submit data should be designed to enable this. Providers should be transparent in all discussions of the data and not withhold information that bears on their accuracy or interpretation. The data collector should be informed promptly if errors are found after data have been submitted.

- Impartiality

Data should be collected, prepared, and submitted with impartiality and objectivity. This process should never be influenced by organisational, political, or personal interests. Higher Education providers should implement controls so that that those who deal with data collections are protected from such interests.

- Rigour

Data should be collected, prepared, and submitted using repeatable and documented processes that can withstand scrutiny. When processes change, records should be kept of previous versions. Estimates and assumptions should be defensible, evidence-based, and documented, and the effect on the data tested. Assumptions and estimates should be reviewed regularly.

Risks

2.1 The university's Risk Register recognises the risks associated with the failure to comply with regulatory requirements. Poor quality data could result in such a failure and give misleading impressions of institutional performance.

2.2 The following risks are associated with the enactment of this Policy:

- There is a risk that the Policy in its written form will not be widely circulated or adopted in practice. To enable its implementation, the Policy should be communicated widely to all staff responsible for data returns on a local level via senior managers.

---

[1] The data collection Codes of practice | HESA

- There is a risk that members of staff involved in the submission of data returns may not be made aware of their responsibilities for enabling the submission of high-quality data. Senior management should encourage all staff to be aware of their individual responsibilities regarding data quality and demonstrate how the maintenance of high standards for data quality is beneficial to their role.

- A lack of clarity on the systems and process relating to data collection, including appropriate training requirement for staff, may lead to inconsistencies in the way that data are collected across the university. Data owners should be encouraged to put clear guidance in place to achieve the highest standards of data quality.

- A regular review of all systems and processes used to support data returns must be undertaken so that reporting requirements are being met and the data collected are fit for purpose.

Scope

3.1 This Policy covers all institutional management data that is held in university-wide systems, and any data that are collected from those systems and used for internal or external reporting. Academic research data collected or used by staff and students are not within the scope of this Policy. Imperial's policy on the use of scientific data can be found via the Research Office[2]. The Audit Commission Report defines data as numbers, words or images that have yet to be organised or analysed to answer a specific question. Information is data in context.

Roles and Responsibilities

4.1 Council

The Council has overall responsibility for the efficient management and good conduct of all aspects of the affairs of the university.

4.2 Audit and Risk Committee

The Audit and Risk Committee is responsible for reviewing the effectiveness of the university's internal control systems. As part of its annual report the Committee is required to give its conclusions on the adequacy and effectiveness of the arrangements for the management and quality assurance of data submitted to the Higher Education Statistics Agency (HESA), HEFCE and other funding bodies.

4.3 President

The President has a general responsibility to the Council for maintaining and promoting the efficiency and good order of the university. As the Accountable Officer, the President is responsible for ensuring compliance with the Office for Students' (OfS) terms and conditions of funding and for providing the OfS with clear assurances about the university's compliance with its regulatory framework. These responsibilities include reporting to the OfS on behalf of the university in relation to its accountability for funding and the quality of its data.

---

[2] Research related policies | Research | Imperial College London

4.4 Registrar & University Secretary

The Registrar & University Secretary leads oversight of data quality. They are a member of and responsible for reporting to the University Management Board.

4.5 University Management Board (UMB)

UMB approves the data quality statement and is responsible for the implementation of policies relating to data quality.

4.6 Heads of department

Heads of department are responsible for the quality of data collected, input and maintained in their departments; for encouraging members of staff to understand the importance of good data and their responsibilities; that appropriate procedures, systems and processes are implemented, clearly documented and communicated to their staff; and that members of staff have the training and competencies required for their roles.

4.7 Members of staff

Members of staff who have responsibility for collecting, inputting and maintaining data are responsible for checking that data is accurate, up-to-date and complete. All members of staff are responsible for recording changes to their personal data in a timely way, either by using the relevant self-service systems or by notifying the appropriate internal department.

4.8 Students

Students are responsible for recording changes to their personal data in a timely way, either by using the relevant self-service systems or by notifying the appropriate internal department.

Policy Statement

5   In order to meet the characteristics of high-quality data outlined above, Imperial has identified the following aims.

5.1 Clearly define responsibility for data quality:

- Individual responsibilities for data collection, storage, analysis and reporting should be defined.

- Every member of staff is responsible for reporting any data quality issues immediately to their manager who should take appropriate remedial action.

- Every member of staff should be aware of policies relating to data quality and related policies (e.g. data protection).

5.2 Enable staff to recognise the need for good quality data, and understand how they contribute towards achieving this:

- Every member of staff should be aware of the implications that poor quality data have both within the institution and externally.

- Staff responsible for data returns should be aware of the purpose of the data they are collecting and their individual role in checking that data meets all requirements and assurances.

5.3 Put in place appropriate policies and procedures:

- The university should define its key data requirements for external returns.

- Every data owner should document the procedures they undertake to collect data for external returns and any local assurance arrangements that are in place.

- All policies and procedures should be reviewed regularly to consider their impact on data quality so that the data collected remains fit for purpose.

- Any changes to policies and procedures should be communicated to all relevant staff.

5.4 Implement systems and processes to secure good quality data:

- Clear systems and processes should be in place for data collection, validation, checking and reporting.

- All data should be internally validated before being submitted externally.

- Data should be collected only once wherever possible to avoid the need for multiple systems. All systems used for data collection should be electronic wherever possible to reduce the risk of human error.

- There should be a clear strategy for the storage of data in line with the Data Protection Policy.

- There should be a regular review of the systems and processes used for data collection, including data warehousing tools so that the data remains fit for purpose.

5.5 Enable staff to have the relevant knowledge and competencies for their roles in relation to data quality:

- All policies, procedures and guidelines should be communicated to staff responsible for data handling.

- Appropriate staff development should be provided to all relevant staff at induction and whenever necessary to encourage all staff responsible for handling data to have the appropriate knowledge and competencies to assure data quality.

- Responsibilities for data quality should be included in job descriptions where data handling is a significant part of the role.

5.6 Subject data to appropriate internal control and verification:

- A regular review of data flows, both institutional and local, should be carried out to assign responsibility for each and establish appropriate levels of control.

- All data should be subject to internal and external audits if deemed necessary.

- Staff responsible for data returns should be able to evidence a full audit trail if requested.

- Staff responsible for producing the return should not be responsible for the final signoff which will be undertaken by a senior manager.

- Any new requests for data held by a department should be referred to the relevant Head of Department and/or the Data Protection Officer.

5.7 The university should have appropriate security measures in place so that data are protected from unauthorised access both internally and externally.

Implementing the Data Quality Policy

6.1 This Policy should be communicated to all relevant staff and displayed on the university website. It is the responsibility of senior managers to make all staff responsible for handling data aware of the Policy and its implications for their work.

Document Control

Document title:		Data Quality Policy	
Version:	V1.1	**Date:**	18/12/2025
Initially approved by and date:		Provost Board 2019	
Version approved by and date:		University Management Board / 8 December 2025	
Version effective from:		December 2025	
Originator:		Division of the University Secretary	
Contact for queries:		Director of Institutional Compliance and Risk Management	
Cross References:		Data Protection Policy Information Security Policy Information Governance Policy Framework	

Notes and latest changes:		2019 – V1.0
		  - Draft created and signed off by Provost Board.
		May 2025 V1.1
		  - Updated branding / document template in line with new branding guidelines.
		  - Removed all references to 'College' as per branding guidelines.
		  - Updated / corrected all URLs, contact details and references/citations where necessary.
		  - Removed / updated references to previous division team names.
		  - Removed reference to Audit Commission in 'Scope' section.
		November 2025 – V1.1
		  - Proposed changes reviewed by Audit and Risk Committee.
		December 2025 – V1.1
		  - Approved by University Management Board.	