St Mary's University Twickenham London

Data Governance Policy

1. Policy

The University operates in an increasingly complex, data-oriented, environment which requires the effective collection, management, analysis and dissemination of data. Institutional data is a strategic asset of St Mary's University. It is critical to University operations that there is appropriate governance for management and use of data. Poor data governance can result in inefficiencies and exposes the University to risk. A consistent, repeatable, and sustainable approach to data governance is necessary to support and protect the integrity of the University's data assets.

This policy introduces a set of standards designed to safeguard the University's position and reputation in relation to published information, alongside building confidence in university data. These standards apply to both quantitative and qualitative data held in the university-wide systems and externally reported.

Data Quality is the result of organisational culture and processes, rather than a single behaviour.

Processes include independent data review and signoff of all externally transmitted data, procedure notes, audit, resilience and backup procedures. These processes should be accompanied by timely and effective staff training, and setting clear responsibilities and ownership.

Note: this policy should be considered alongside the University's policy on GDPR.

Terminology

Data or Institutional Data is a general term used to refer to the University's information resources and administrative records.

Data Quality refers to the validity, relevancy, accuracy and currency of data.

Data Trustee is accountable for the strategic co-ordination of data management and reporting.

Data Owner *is* accountable for the fitness or purpose of a defined data area. This role is primarily performed by the leads of those functions.

Data Steward is responsible for the definition and quality of defined dataset(s) within a data area, wherever that data is retained. Responsible for determining the relevant data quality checks and controls to maintain data quality in line with the university's operational and strategic needs.

Data Custodian is responsible for the safe custody, storage and retention of data.

Data User is any member of staff who uses data in the normal course of business. They can expect that such data is valid, relevant and current but is expected to raise any perceived shortfalls with the data owner.

2. Scope of the Policy

The scope of this policy covers all data held in enterprise systems (including the collection of data into those systems from internal or external sources) and any data used from those systems for internal or external reporting. The policy does not cover data held by the University where the data owner is a third party, such as student coursework.

Corporate data that are used to inform analysis and reporting do not all reside in enterprise systems. However, there is a long-term intention to align all data systems. Some of the data within scope of this policy may exist in local databases and on spread sheets.

This policy applies to all members of staff who use data in the normal course of business.

This policy applies to both quantitative and qualitative data held in university-wide systems and externally reported data.

Research data is in scope where it is stored in the University's research data repository-'Open Research Archive' for long term access, primarily to meet open data requirements and support publication of research results. Active research data is not in scope.

4. Roles and Responsibilities

4a. Governance & Leadership

St Mary's University, rather than any individual or Organisational Unit, is the owner of all institutional data. As such, the University will require a culture that demonstrates a high commitment to data quality at a senior level. All members of SLT have a strategic responsibility for maintaining good data quality.

Every member of staff who interacts with data at every level within the University has a role to play in the improvement of data accuracy, quality and completeness in compliance with University requirements.

Individuals often play multiple roles at the University and certain staff have roles defined within the data governance policy. Together these role holders form the University's data stewardship community.

To be effective each role in the data stewardship community must have unambiguous, easily understood and publicly documented responsibilities and where appropriate these will be incorporated into job descriptions so that the identified responsibilities form part of substantive University posts rather than parallel activities.

The University's Board of Governors hold ultimate responsibility for data quality assurance, however, it is the responsibility of individual members of staff to ensure that the principles of this policy are followed to maximise the accuracy and timeliness of data used internally and reported externally.

4b. Data Governance

The Risk Management Group (RMG) is a University-wide Group responsible for overseeing the effective implementation of the University's Data Governance Policy. The Group also assures appropriate data processes are used in all of the University's data creation, use and dissemination. Where separate groups are established to confirm data assurance, it is expected that they will operate in accordance with University policies and procedures.

The ***Data Trustee*** is accountable for the strategic co-ordination of data management and reporting. The Data Trustee will be a member of SLT and have ultimate accountability for individual data sources.

Every data source must have a ***Data Owner*** (see below) who is responsible for the quality, integrity, implementation and enforcement of data management within their Organisational remit and ensuring data meets internal and external quality, accuracy and submission requirements.

Data Stewards are responsible for ensuring effective local protocols are in place to guide the appropriate use of data, wherever that data is retained or published. They will also ensure that, wherever possible, data has a single point of origin and that other uses are derived from this single point of origin (a single version of the truth). The Data Steward, having determined the category of the institutional data as confidential, will approve access based on appropriateness of the ***Data User's*** role and its intended use. Where necessary, approval from the ***Data Owner*** may be required.

The ***Data Custodian*** is responsible for the safe custody, storage and retention of data. The data custodian will ensure that appropriate security arrangements are in place to protect data from unauthorised access both internally and externally.

Data	Data trustee	Data Owner	Data Steward
Staff data	COO Deputy Vice Chancellor	Director of HR & Legal Services	Head of HR Operations
Student data (applications)	Provost	Director of IESRA	Head of Admissions
Student data (enrolments)	COO Deputy Vice Chancellor	Director of Student Operations	Academic Registrar
Academic Programme data	Provost	Dean of Education & Outcomes	Academic Registrar
Research data/publications	Provost	Provost	Head of Research Services
Finance data	CFO- Pro Vice Chancellor (Enterprise and Chief Financial Officer)	Financial Controller	Head of Accounting Services
Estates data	COO Deputy Vice Chancellor	Director of Estates & Campus services	Senior Asset Manager

The Data Custodian will be the Chief Information Officer (CIO), where the information is held in electronic form or within the University's IT systems. The CIO and the CIO's team are not a data owner or steward.

5. Objectives for Data Quality

St Mary's University needs complete, accurate and reliable information in order to manage its business, including:

- Delivering an efficient service to staff, students and stakeholders
- Providing informative and reliable management information and reporting
- Demonstrating public accountability
- Presenting a responsible and true public face
- Meeting statutory and regulatory obligations

The principal reasons why data reported *externally* should be of the highest possible quality are:

- The external representation of the University has assumed greater significance in the context of increased tuition fees. It is imperative that we provide students, and potential students with clear, accurate data that can help inform their decision-making.
- To ensure accurate funding allocations for both teaching and research (data supplied by the University to the Office for Students [OfS] and the Higher Education Statistics Agency [HESA] affects the funding the University receives).
- Good quality data and external returns reflect a well-run institution and this is likely to increase the University's external credibility.
- The University's Risk and Audit Committee is required to give, as part of its annual opinion, assurance over management and quality assurance of data submitted to HESA, the OfS and other external agencies.
- The University's senior management are required to provide representations in the annual audited financial statements that internal controls are effective, including assurance over data quality.

6. Data Quality Principles

The data quality principles should aid the creation of a strong data quality culture across the University and lie at the heart of our approach to data quality. Each principle is accompanied by a set of practices which support their adoption. (Please refer to 'Data Quality Principles in appendix B)

The principles are:

- Commit to data quality
- Know your users and their needs
- Assess quality throughout the data lifecycle
- Communicate data quality clearly and effectively
- Anticipate changes affecting data quality

7. Data Scrutiny & Review

The need for data should be periodically reviewed to ensure the data is necessary and that it is collected in the most efficient means possible. Where possible, data held on university systems should be:

- Subject to on-line validation at the point of entry
- Subject to verification by the data subject (where appropriate)
- Represented by a single point of origin.

Data should be entered once and in the formally agreed system of record. Then, when needed by other systems, data should be extracted or referenced in as near real time as possible. Where a system of record has been agreed for a particular data source (e.g. student term time address) that data should not be entered in any other system. Rather it should be referenced or extracted in as near real time as possible.

Data should wherever possible be held in a university-managed system and local spreadsheets for holding data should not be used. Data should not be downloaded from systems and held locally unless there is an explicit business need

All data held on University systems should be scrutinised on a regular basis for reasonableness, accuracy and fitness for purpose to identify possible data errors or missing values. The Data Owner is responsible for ensuring that the appropriate checks are undertaken.

Data Stewards should pay particular attention to the dimensions of data quality:

1. Completeness: meaning there are no gaps in the data from what was supposed to be collected to what was collected. This means that essentially everyone on your team is reporting a full set of data.
2. Consistency: everyone is collecting data in the same way. The goal here is for everyone who collects data to have the same understanding of what to fill in on data collection forms and as part of processes.
3. Accuracy: The data recorded is correct and free of errors.
4. Timeliness: The information available when you need it.
5. Validity: Information is in a specific format and follows business rules.
6. Uniqueness: Data is not duplicated and only one instance in which the information appears in the database.

8. External returns

Data Owners should undertake a thorough assessment of the data to be reported externally well in advance of the submission deadline. The relevant Data Owner should evaluate summary statistics for any data set returned externally:

- For reasonableness; and
- For context in terms of summary statistics for previously submitted data.

At the final data review and sign off the responsible Data Trustee must undertake a high level check for credibility and reasonableness before recommending to the Vice-Chancellor that the return should be signed-off. Any external return being submitted to the Vice-Chancellor for sign-off should be accompanied by a Data Assurance Form (see appendix A).

Procedure notes should be compiled for each external return. Procedure notes should be user friendly and accessible to other members of staff within the University. These should be reviewed periodically and updated to reflect the most recent guidance and practice. The Data Owner and Director of Strategic Planning (where the return is being compiled by the Student Returns Manager) must ensure that these procedures are adopted and embedded within working processes to guarantee compliance.

Data returns are formal reports of University data to external agencies for regulatory or statutory purposes, or for accreditation or funding purposes. Organisational resilience should be delivered by ensuring that data returns can be completed by at least two competent and fully trained members of staff – preferably each with practical experience of completing and preparing the data return. This will reduce the University's exposure to risk in the event of staff unavailability.

Staff responsible for undertaking data returns should be appropriately trained in the necessary technical skills to undertake the work and be given an understanding of the context and specifics of the return. Responsibilities for data accuracy should be included in the job descriptions for those staff with significant management responsibility or where data handling is an important part of the role.

All members of staff should understand their role in contributing to good quality data, as well as their individual responsibilities, and be aware of the implications of poor data quality both within the institution and externally. Members of staff should be encouraged to immediately report data quality issues to their manager. The manager will undertake appropriate action to remedy the situation, escalating concerns to the appropriate level within the organisation (usually Head of School/Service). Data quality issues which may have a significant financial or reputational impact should be reported to the University Risk and Audit Committee via the University Secretary.

The University Secretary & Director of Strategic Planning will maintain a list of regular data returns made to external organisations and will be required to review each external return before it is submitted to ensure accuracy and consistency across returns.

9. Breach and Non-compliance

Any issues in the first instance should be referred to the Data Steward and the Data Quality Manager. The Data Quality Manager will maintain a log of all data issues, the proposed plan for resolution and the timeline for doing so. If a data quality issue is not satisfactorily resolved then this should be escalated to the Data Owner and ultimately to the Data Trustee. If the issue is still not satisfactorily resolved then this should be reported to the Risk Management Group and ultimately to the Risk and Audit Committee if concerns are not adequately addressed.

10. Data Security and Storage

Compromised data availability negatively impacts the day-to-day delivery of business services and the ability of the University to deliver its strategic objectives.

Technical security measures for data storage should match the requirements of the information classification.

All members of the data community have a responsibility to report any compromise of systems or data to the University Data Protection Officer immediately. (GDPR@stmarys.ac.uk)

11. Training and Education

The University will foster a culture of education and data literacy to support the data quality requirements defined in this policy.

The RMG will ensure that data governance and management training as part of staff induction and continuous staff development are available for all Data Stewards.

The Data Quality Manager will develop and deliver educational materials to support data quality issues and wherever possible provide training to data stewards

Date Written	**December 2024**
Author	Director of Strategic Planning & Data Quality Manager
Version number	V2.1
Person responsible	Director Strategic Planning
Effective from	December 2024
Review date	August 2025
Impact Assessment date	
History (where discussed / who circulated to / committees considered	Risk Management Group, University Executive Committee

Appendix A. External Return Assurance Form

Statutory Return Data Assurance Form
Statutory Return:
Compiled By:
Reviewed By:
Date of submission:

Brief description of return
Provide a brief summary of the return, including the purpose of the return, to whom the return is submitted, the data covered in the return, and the time period to which the return relates.
Summary of key outcomes of return
Provide high level outcomes from the return including headline figures. Highlight any significant changes from the previous year and likely impact on internal and external factors.
Improvements made since last return
Highlight any actions taken to improve the return, particularly focusing on steps taken to address issues raised in last year's return.
Key changes to guidance
Outline any material changes to the guidance for completing this return and confirm that the necessary steps have been taken to meet changes.
Data integrity
Outline the data quality and validation checks that have been undertaken in order to ensure that the data is accurate and robust
Impact assessment
Outline the likely impact of the data submission on external publications, funding allocations or the University reputation.
Risk assessment
Give an overall assessment of the level risk associated with this data return.
Key actions for next return
Outline any changes you would like to see to the process of collecting and checking the return.

APPROVAL
I confirm that the information provided in the attached statutory return is accurate, presenting a reasonable and accurate view of the University. I recommend that the Statutory Return is signed by the Vice-Chancellor.

Prepared by: Signature Date	Approved by (Head of Service): Signature Date

Appendix B. Data Quality Principles

Data quality principles

These principles should aid the creation of a strong data quality culture across the University. This detailed document expands on the principles setting out good practice, procedures and attitudes that will be most helpful to ensuring our data is fit for purpose.

These principles should lie at the heart of our approach to data quality. Each principle is accompanied by a set of practices which support their adoption.

The principles are:

- Commit to data quality
- Know your users and their needs
- Assess quality throughout the data lifecycle
- Communicate data quality clearly and effectively
- Anticipate changes affecting data quality

1. Commit to data quality

Data trustees must create a sense of accountability for data quality across their team(s) and make a commitment to the ongoing assessment, improvement and reporting of data quality.

1.1 Embed effective data management and governance

Fit for purpose data depends on effective data management and governance practices.

Data owners should:

- adopt formal data governance practices to ensure that data is managed properly
- adhere to agreed data principles
- apply data standards to ensure that data is reusable and interoperable
- guide an organisation or team's strategic direction by ensuring awareness and improvement of data quality

Data stewards should:

- ensure that measuring, communicating and improving data quality is at the forefront of activities relating to data

1.2 Build data quality capability

The Data Quality Manager should:

- dedicate time and resource to building capability in assessing, improving and communicating data quality through training and sharing best practice

- include best practice in data quality management (such as the data quality dimensions) as part of training materials

1.3 Focus on continuous improvement

Continuous improvements can help to avoid data quality problems before they occur.

Director of Strategic Planning should:

- benchmark and regularly assess levels of data quality over time to track changes in quality
- prioritise and iterate effective improvements to achieve fit for purpose data
- use data quality action plans to identify and define where efforts should be prioritised

2. Know your users and their needs

Understanding user needs is essential to ensuring that data is fit for purpose. Data owners should research and understand users' needs, prioritising efforts on the data which is most critical.

2.1 Research your users and understand their quality needs

To achieve fit for purpose data, it is essential to understand your users' quality needs.

Data stewards should:

- proactively and regularly engage with users to understand their priorities
- carry out additional research if faced with a large, complex or poorly understood group of users
- capture a range of user needs for data which has multiple uses
- balance the conflicting needs of users where possible and prioritise improvements which have the greatest impact
- regularly communicate with users to understand any changes in their requirements

3. Assess quality throughout the data lifecycle

Data should be managed across its lifecycle, paying close attention to quality measures and assurance at each stage.

3.1 Assess data quality at all stages of the lifecycle

Quality assurance should take place across the entire data lifecycle. Data quality issues can occur at any stage and can have knock-on effects for the rest of the lifecycle.

Data stewards should:

- assess data quality at every stage and take proactive measures to improve quality when issues arise
- adopt appropriate assessment measures at each stage rather than applying a one-size-fits-all approach to quality assurance
- focus quality improvements as early in the lifecycle as possible to maximise their effectiveness

3.2 Communicate with users and stakeholders across the lifecycle

Different stakeholders will often be involved across the data lifecycle.

Data stewards should:

- develop effective communication channels with and between stakeholders to ensure a broad understanding of data quality
- communicate any changes in data quality to stakeholders at all stages of the lifecycle
- proactively engage with data providers to ensure a clear understanding of data quality requirements

4. Communicate data quality clearly and effectively

Communicate quality to users regularly and clearly to ensure data is used appropriately.

4.1 Communicate data quality to users

The Data Quality Manager should:

- provide clear data quality information and describe its impact on use of the data
- communicate trade-offs in data quality clearly to aid understanding of the data's strengths and weaknesses
- be transparent about the quality assurance approach taken and communicate data quality issues clearly to users
- build strong relationships with data stewards and users to identify data quality problems at source
- provide clear definitions of terminology used and not presume a high level of user understanding of data quality

Data stewards should:

- inform users in advance about changes made to data processes which could impact on quality
- communicate clearly and in plain language, following relevant style guides for published materials

4.2 Provide effective documentation and metadata

Data stewards should:

- document and share **metadata** to minimise ambiguity and enhance opportunity for data access and reuse
- document and report data quality issues and be transparent about steps being taken to address them

5. Anticipate changes affecting data quality

Not all future problems can be predicted. Where possible, anticipate and prevent future data quality issues through good communication, effective management of change and addressing quality issues at source.

5.1 Plan for the future

Members of the DGG should:

- use root cause analysis to solve data quality issues at source, rather than apply temporary fixes
- regularly communicate with users to keep up with changing data and quality requirements
- proactively consider the impact of changes in systems on data quality
- integrate quality processes into the design of new data systems
- ensure metadata and other supporting documentation is thorough and up-to-date
- Regularly review statutory and regulatory requirements to ensure compliance

Dimensions of data quality

Completeness: meaning there are no gaps in the data from what was supposed to be collected to what was collected. This means that essentially everyone on your team is reporting a full set of data.

Consistency: everyone is collecting data in the same way. The goal here is for everyone who collects data to have the same understanding of what to fill in on data collection forms and as part of processes.

Accuracy: The data recorded is correct and free of errors.

Timeliness: The information available when you need it.

Validity: Information is in a specific format and follows business rules.

Uniqueness: Data is not duplicated and only one instance in which the information appears in the database.