



University of  
St Andrews

## Data Governance policy

|                                   |                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------|
| <b>Document type</b>              | <b>Policy</b>                                                                   |
| <b>Scope (applies to)</b>         | Staff and students                                                              |
| <b>Applicability date</b>         | 29/07/2025                                                                      |
| <b>Expiry date</b>                | 28/07/2026                                                                      |
| <b>Approved date</b>              | 13/08/2025                                                                      |
| <b>Approver</b>                   | Assistant Vice-Principal (Strategy and Planning)                                |
| <b>Document owner</b>             | Head of Data Governance                                                         |
| <b>School / unit</b>              | IT Services                                                                     |
| <b>Document status</b>            | Published                                                                       |
| <b>Information classification</b> | Public                                                                          |
| <b>Equality impact assessment</b> | None                                                                            |
| <b>Key terms</b>                  | Information governance and management/Data governance                           |
| <b>Purpose</b>                    | The Data Governance policy defines the University framework for governing data. |

| <b>Version number</b> | <b>Purpose / changes</b>                                                                                                                                  | <b>Document status</b> | <b>Author of changes, role and School or unit</b> | <b>Date</b> |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---------------------------------------------------|-------------|
| 4                     | Changes to improve alignment with related University policies and practices for Intellectual Property, Research Data Management and Digital Preservation. | FINAL                  | Head of Data Governance                           | 30/07/2025  |

- British Sign Language (BSL) users can contact us via the online BSL Video Relay Interpreting Service: <https://contactscotland-bsl.org>
- This document and forms associated with this document are available in an alternative format upon request.

## Contents

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| 1. Purpose .....                                                                | 3  |
| 2. Definitions.....                                                             | 3  |
| 3. Requirements .....                                                           | 6  |
| 4. Risks and threats.....                                                       | 6  |
| 5. Scope and success .....                                                      | 7  |
| 6. Principles .....                                                             | 8  |
| 7. Data governance framework.....                                               | 8  |
| 8. Roles and responsibilities in the data stewardship community.....            | 9  |
| 9. Data assignment .....                                                        | 12 |
| 10. Data quality capability.....                                                | 13 |
| 11. Data quality oversight .....                                                | 14 |
| 12. Training and education .....                                                | 14 |
| 13. Data security.....                                                          | 15 |
| 14. Communication and review .....                                              | 15 |
| 15. Related documentation .....                                                 | 16 |
| 16. Appendix 1 – The six characteristics or dimensions of data quality.....     | 17 |
| 17. Appendix 2 - Data principles .....                                          | 19 |
| 18. Appendix 3 - Roles and responsibilities of the data stewardship community . | 21 |
| 19. Appendix 4 - Responsibilities of the Data Governance Operations Group.....  | 1  |
| 20. Version Control .....                                                       | 2  |

# 1. Purpose

- 1.1. The University of St Andrews needs high-quality data to manage its activities, sustain its ambitions for future growth, drive innovation and meet its obligations to demonstrate accountability through accurate reporting and evidence-led decision-making.
- 1.2. Individuals and functions within the University rely on shared data, so data governance requires management activities that treat corporate data as an asset owned by the institution rather than by organisational structures.
- 1.3. To treat corporate data as an asset, it is essential that everyone who works for the University understands their role in relation to the data they create or use throughout the information life cycle.
- 1.4. As an evidence-led institution, the University is committed to creating a culture and an accountability framework that share understanding of, and sensitivity for the value of the institution's data assets.
- 1.5. Data availability, data accessibility and data quality are measures of good data governance. This policy describes the University's approach to data governance in those terms and outlines how clear accountability for each measure is managed.

## 2. Definitions

- 2.1. For this policy the following definitions apply:
  - 'Data' is defined as 'numbers, words or images that have yet to be organised or analysed to answer a specific question.'
  - A 'data asset' represents the source data along with associated metadata.
  - 'Corporate data' means data collected, generated, or received by the University for the purposes of operational or management information reporting.
  - 'Data accessibility' refers to the retrieval of data in an

authenticated manner approved by the University. This may be for the purposes of reading, modifying, copying or moving data from a system. The term in this context has no reference to disability or related arrangements.

- A 'data domain' is a large set of data related to a particular business area such as Admissions, Registry, Finance, Estates, Development. Although data domains may often appear to map to the University's organisational hierarchy they need not do so. Data domains may comprise smaller sets of data known as sub-domains if the need arises.
- 'Data governance' includes the people, processes and technologies used by the University to manage and protect its corporate data assets including definitions for how the institution assigns accountability and control over the assets and their use.
- 'Data linkage' is the supplementation of one data set with another at the same level of granularity or the pairing of records from different data sources.
- 'Data literacy' is the 'ability to read, write and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied — and the ability to describe the use case, application and resulting value'. Definition from the Gartner Glossary. Last accessed 24<sup>th</sup> February 2025 at <https://www.gartner.com/en/information-technology/glossary/data-literacy>.
- 'Data quality' refers to:
  - data that satisfy the expectations of stakeholders across the dimensions of accuracy, validity, reliability, timeliness, relevance, and completeness. (see Appendix 1 for more information).
  - And the processes used to measure or improve the quality of data.
- 'Data security' includes data confidentiality, data integrity, and data accessibility. See section 13 below.
- The 'Data Warehouse' is the University's central ITS-maintained repository for data used for management information reporting or applications integration.

- ‘Deposited’ data refers to a type of research data archived and managed within a disciplinary, funder or institutional repository that supports recognised standards for access, sharing and publication.
- ‘Enterprise’ is used to qualify aspects of infrastructure which are University-wide and, although not exclusively so, centrally managed by IT Services.
- ‘Information lifecycle management’ “is an approach to data and storage management that recognises that the value of information changes over time and that it must be managed accordingly.” Definition from Gartner Glossary. Last accessed 24<sup>th</sup> February 2025 at <https://www.gartner.com/en/information-technology/glossary/information-life-cycle-management-ilm>.
- ‘Personal data’ refers to the data covered by the UK General Data Protection Regulation when read with the Data Protection Act 2018. The Data Protection Laws outline principles for the collection and management of personal data. While not all data processed by the University are personal data, application of the data protection principles, and other recognised standards and practices for data management provide a framework for assuring the accuracy, integrity, quality and sustainability of institutional data assets.
- ‘Reference data’ is any ‘data used to characterise or classify other data, or to relate data to external information.’ Definition from the DAMA DMBoK, 2nd edition, 2017, 10.1.3.2.
- ‘Research data’ refers to data created by or used for research at the University. Research data are defined as the data, objects, materials or artefacts needed to reproduce/retrace the published outcomes of research, whether physical or digital. Research data is further classified as three types: active, archive and access.
  - active data are actively part of the research process and are not in scope.
  - archive data are all data requiring secure, long-term preservation, including confidential or sensitive data.
  - access data are a subset of archive data and are data deposited in Pure to support access, sharing and publication).

### **3. Requirements**

- 3.1. The University must ensure the availability and quality of its data assets to:
- enable the creation of information that is fit-for-analysis, fit-for-purpose, relevant, and right for context
  - produce accurate and reliable management information on which timely, informed corporate decisions can be made
  - provide effective and timely services to students, staff, and other stakeholders
  - monitor and review business activities and operations
  - evaluate and control costs of business (research, education and corporate) operations
  - produce accurate external returns for funding and benchmarking purposes
  - demonstrate accountability to public and private regulators and sponsors
  - foster a data-driven business orientation
- 3.2. The requirement to maintain good data availability and quality is covered by legislation such as the Data Protection Act 2018 (with UK GDPR from 1 January 2021). Funding bodies such as the Scottish Funding Council (SFC) and other external bodies such as the Higher Education Statistics Agency (HESA), the Research Excellence Framework (REF) and UK Research and Innovation (UKRI) place quality requirements on the University over the data that are to be transferred to them so they can carry out their statutory duties.

### **4. Risks and threats**

- 4.1. The corporate health of the University suffers when the value of its data assets depreciates through a loss of relevance, asset management standards or shared understanding.
- 4.2. This can happen through poor regulation or infrastructure, deficient data availability, lack of capability to perform data linkages, erosion in data quality and/or disconnection between staff responsible for data collection vs information creation.
- 4.3. Symptoms of poor corporate health are evidenced in enhanced risks such as:

- inadequate reporting to funders and sponsors:
    - under-reporting resulting in financial penalties, sanctions, or funding shortfalls
    - over-reporting resulting in over-payments and subsequent financial clawbacks
  - ill-informed decision-making or inappropriate corporate conclusions
  - reputational damage in areas such as student access, recruitment, retention, and attainment
  - misrepresenting performance in teaching and research
  - loss of productivity due to time spent on non-value-added tasks
- 4.4. Some symptoms may go unnoticed for periods of time. This is especially true of inadequate reporting where inaccurate, inconsistent, out of date, incomplete, missing, or misinterpreted data can accrue in corporate systems before being used to create information.

## **5. Scope and success**

- 5.1. The successful implementation of this policy will primarily be evidenced through the governance of data domains (such as curriculum, estates, finance, staff, student) represented in the University's enterprise Data Warehouse; however, this policy is not limited to data in the Data Warehouse.
- 5.2. The scope of this policy includes data used for operations or to inform analysis and reporting, including statutory reporting, whether data are collected by the University or gathered from partners or external sources.
- 5.3. 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.
- 5.4. Corporate data that are used to inform analysis and reporting do not all reside in enterprise systems, but this remains a long-term ambition; consequently, some of the data within scope of this policy may exist in local systems such as MS Access databases or spreadsheets.

- 5.5. Research data are in scope where they are deposited in the University's research data repository for long term access and preservation primarily to meet open data requirements and support publication of research results, and/or archived in a system for preservation purposes.
- 5.6. Active research data (in use during project lifecycles) are not in scope.
- 5.7. In all cases research data are owned by researchers and the University has a responsibility for systems, metadata and processes to support good research data management.
- 5.8. Successful delivery of the objectives in this policy relies on the application of data security arrangements to protect data from unauthorised access from outside the University.

## 6. Principles

- 6.1. Principles are a key element in the structured processes that collectively define and guide the University, from values through to actions and solutions.
- 6.2. The principles in Appendix 2 should be applied to the management of all corporate data within the University and should also be applied to associated operational processes, goals, and staff training.
- 6.3. Exceptions to these principles must be documented and visible even when principles allow for exception handling (for example "Data should be collected and recorded once only *wherever possible* without the need for multiple systems").

## 7. Data governance framework

- 7.1. Data governance is needed to guide and facilitate information technology, data processes, and decision-making to support the University in reaching its goals. Good data governance is only meaningful when it aligns with institutional goals and values in a sustainable manner.
- 7.2. The University is committed to ensuring that a sustainable data governance framework exists to achieve good data accessibility, availability and quality and to mitigate against associated

potential risks.

- 7.3. In response to its commitment, the University has adopted a framework built on the concept of community stewardship with clear lines of accountability.
- 7.4. Sustainability is achieved by nurturing staff competencies based on a common set of best practices in data management across the institution with special attention paid to consistency in approach at all levels of engagement.
- 7.5. The data governance framework enables a coherent approach to the development, curation and oversight of institutional reference data (for example organisational hierarchies).
- 7.6. To ensure successful adoption a data governance policy must be published and familiarised at all levels across the University along with relevant targeted training.
- 7.7. Good data governance should mature and adapt to the institution's changing needs and processes. The management and implementation of data availability and data quality activities requires experience and expertise, and the University is committed to ensuring enough resources are available to enable the delivery of this policy to the highest standard.

## **8. Roles and responsibilities in the data stewardship community**

- 8.1. Every member of staff who interacts with data at any level within the University has a role to play in the improvement of data accuracy and completeness in compliance with University requirements.
- 8.2. Individuals often play multiple roles at the University and certain staff have roles defined within the data governance framework. Together these role holders form the University's data stewardship community.
- 8.3. 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 or satellite activities.

- 8.4. The information life cycle recognises different relationships to data. **Data producers** (whether people or systems) control the data they create. Sometimes data are created for one purpose but are used for other purposes by **data consumers**. Because data producers have knowledge of the purposes and functions of associated processes, they own they can modify processes to ensure they meet the needs of data consumers.
- 8.5. Any person (or system) who has access to institutional data is a **data consumer** therefore data consumers encompass most University staff whether they contribute directly to data collection or edits. Data consumers have a responsibility to follow established guidelines for accessing, sharing, and updating data as well as participate in activities that define data for use.
- 8.6. **Individual researchers** are responsible for creating data management plans to include collection, retention, storage and/or sharing solutions; and for depositing to appropriate archives. The quality of research data (in common with research outputs including theses and accepted manuscripts) is the responsibility of individual researchers.
- 8.7. The data governance practice at the University is formalised through the close and collective working of the **Assistant Vice Principal (Strategy & Planning)**, **Head of Information Assurance and Governance** and the **Head of Data Governance**. Together these three roles provide coherence for the institutional data governance function because they have responsibilities associated with compliance, are accountable for ensuring business needs are addressed, and bring oversight to, and ensure delivery of the data principles.

| <b>Role</b>                                    | <b>Summary responsibilities</b>                                                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assistant Vice Principal (Strategy & Planning) | set and approve institutional reporting requirements and approve the associated methodologies for transforming corporate data for the purpose of reporting                                                  |
| Head of Information Assurance and Governance   | advise on and/or support the creation of policy, procedures and governance arrangements for the management of personal data and its lawful use including the sharing of personal data with external parties |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Head of Data Governance | ensure institutional business needs can be met through corporate data structures; set and oversee data governance frameworks and standards; oversee the delivery of the data governance policy; manage the activities of the Data Governance Office (DGO); Data Governance Operations Group (DGOPs Group); and facilitate collaborative activities in the data stewardship community, including the Data Assets Management Group (DAMG) |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 8.8. Accountability and responsibility for delivering the activities defined in this policy lies with an institutional network of staff in data ownership and data stewardship roles. (Appendix 3 provides a full list of responsibilities for the roles identified in the framework.)
- 8.9. **Data owners** will typically be senior managers with responsibility for business operations. By default, Heads of Units are named as data owners in their Job Descriptions. They have responsibility for challenging metadata quality and/or data quality; consequently they are accountable for the accuracy and completeness of data and information within their data domain(s).
- 8.10. Ownership of research data remains with individual researchers, with the University providing support for stewardship of archived research data and its associated metadata.
- 8.11. Data accessibility arrangements for domain data are the responsibility of data owners except in the case of research data where data stewards have responsibility for accessibility arrangements where the data have been deposited by data owners.
- 8.12. **Data stewards** carry out their responsibilities on behalf of data owners. Data stewards will be nominated by data owners (or in the case of research data will carry out this role by default on archived data) and will typically be subject matter experts or team leaders with responsibility and oversight of processes and people who interact with corporate or research data. They have responsibility for the accuracy and quality of metadata, data and information within specific data domains, for undertaking data quality checks where appropriate and for identifying and implementing data quality improvement measures.
- 8.13. Research data stewards will have responsibility for metadata standards and integrity of data files where these have been

deposited into a system for access and/or preservation purposes.

| <b>Role</b>  | <b>Summary responsibilities</b>                                                                                                                                                                                                                                                          |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data owner   | ensure compliance; act as escalation point for matters relating to data governance in their domain; manage, protect, and ensure the integrity and usefulness of University data; ensure data improvements are implemented; authorise user access requests where there is legitimate need |
| Data steward | implement data standards; monitor data quality in their domain; manage enquiries about domain data and monitor usage; participate in Data Assets Management Group (DAMG) activities                                                                                                      |

8.14. Data stewards collaborate in the **Data Assets Management Group (DAMG)** which provides a forum to highlight data domain issues, seek support and assess the impacts of local changes on corporate data.

8.15. All role holders in the data stewardship community will be supported by a **Data Governance Office (DGO)** which comprises the **Head of Data Governance** and **Data Governance Officer**, and the **Data Governance Operations Group (DGOps)** which comprises the DGO as well as representatives and stakeholders from across the University that provides a point of institutional contact and an advisory service for data-related activities (see Appendix 4). The DGO and DGOps Group have a co-ordinating function to support consistency of practice, enable data governance exception handling and plan the delivery of related training requirements. In addition, the DGO has responsibility for managing the change request process in relation to the Data Warehouse. (**Appendix 4** provides a full list of responsibilities.)

## 9. Data assignment

9.1. Each corporate data domain is assigned a data owner and, where expedient, a data steward.

9.2. Where possible a single owner of corporate data will be assigned but where this is not possible or desirable then ownership at a lower level will be established to avoid multiple ownership.

- 9.3. Data aggregations and summaries in the Data Warehouse will be assigned an owner based on publication or visualisation requirements.
- 9.4. The methodologies used to transform data in the Data Warehouse will be assigned an owner, often the Director of Planning if the transformations are for institutional reporting.

## **10. Data quality capability**

- 10.1. The University will develop its technical infrastructure capability to enable data owners to monitor and measure data quality in their data domains.
- 10.2. The University will be able to monitor the corporate health of data identified for use in the Data Warehouse as they are captured and transformed by systems and processes. Specific attention will be given to the availability of data for use in cross- institutional aggregations of data for reporting.
- 10.3. This capability will be supported across multiple layers of the institution by automations and software and will include data both before and after consumption by the Data Warehouse.
- 10.4. Successful implementation of this data quality capability will be evident through:
  - successful delivery of the data governance framework
  - proactive measuring against the six characteristics or dimensions of good data in Appendix 1
  - the use of data quality flags and reports maintained by data stewards and visible to data owners
  - continuous data quality monitoring and data improvement activities focussed on the Data Warehouse
- 10.5. The delivery of the University's data quality capability will be overseen by the Head of Data Governance supported by the DGO who will support data owners in relation to the co-ordination and delivery of relevant activities especially in relation to data consumed by or created in the Data Warehouse.

## 11. Data quality oversight

- 11.1. High-quality data originate from a culture that understands the importance of data accuracy and that is embedded in the institution's operational, performance and governance arrangements. A mature organisation demonstrates its ability to meet the need for high-quality data by thinking holistically and having the correct processes, systems, responsibilities and training in place to ensure appropriate data management and governance through relevant roles that collaborate.
- 11.2. The strategic oversight of corporate data quality including the definition of current data quality metrics and the forecasting of future needs is the collective responsibility of the Assistant Vice Principal (Strategy & Planning), Head of Information Assurance and Governance and Head of Data Governance.
- 11.3. Together these three roles act as a **Data Steering Group** that will:
- collaborate with data owners on external requirements
  - communicate with senior leaders the expectations and requirements of data governance described in the policy
  - identify and prioritise strategic data quality initiatives
  - arbitrate on differing practices of data quality management
  - guide data management and instruct data operationalisation activities
- 11.4. The Data Steering Group reports into the Business Design Authority (BDA) which safeguards the University's enterprise architecture capability.

## 12. Training and education

- 12.1. The University will foster a culture of education and data literacy to support the data quality requirements defined in this policy.
- 12.2. The DGO will ensure that data governance and management training as part of staff induction and continuous staff development are available for all role holders in the data stewardship community.
- 12.3. Wherever possible, training will be delivered on a cyclical basis (for example all staff are required to complete data protection

training once every 3 years).

- 12.4. The DGO and DAMG will develop and deliver educational materials to support data quality issue analysis and remediation.
- 12.5. The DAMG will provide a forum for data stewards to support the communication and adoption of good practice in relation to data quality.

## **13. Data security**

- 13.1. For the University to function, innovate and demonstrate compliance with security legislation data must be readily available.
- 13.2. Compromised data availability negatively impacts the day-to-day delivery of business services and the ability of the University to deliver its strategic objectives.
- 13.3. Data availability in relation to data classification and user accessibility is governed by relevant other University policies. It is the responsibility of data owners to ensure that data have a classification based on the information classification policy. See below Section 16.
- 13.4. Technical security measures for data storage should match the requirements of the information classification.
- 13.5. Data availability is a shared responsibility between IT Services and data owners supported by the DGO.
- 13.6. All members of the data community have a responsibility to report any compromise of systems or data to the University incident response team ([stacsirt@st-andrews.ac.uk](mailto:stacsirt@st-andrews.ac.uk)) and the University Data Protection Officer ([dataprot@st-andrews.ac.uk](mailto:dataprot@st-andrews.ac.uk)) as soon as possible.

## **14. Communication and review**

- 14.1. This policy will be published online via the University Governance Zone and will be communicated to stakeholders publicly via the University website [www.st-andrews.ac.uk](http://www.st-andrews.ac.uk).

14.2. The University's data requirements will change over time. Regular review will ensure ongoing dialogue with users in the University and external communities. This policy will be reviewed at least annually to keep pace with those conversations and the maturity of experience. If there are periods of rapid change this policy will be modified as needed to reflect current priorities, infrastructure, research, or investment.

14.3. This policy applies from the date of publication.

## 15. Related documentation

15.1. University of St Andrews information can be found at:

- [Regulations governing the use of University information and communications technology \(ICT\) facilities](#)
- [Information classification policy](#)
- [Research Data Management policy](#)
- [Privacy and data protection webpage](#) with links to notices, guidance and related links

15.2. External information

- [Data Protection Act 2018](#)
- HESA Reporting. For example, the [Student Data Quality Report](#)

## 16. Appendix 1 – The six characteristics or dimensions of data quality

### 1. 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

### 2. Validity

- Data should be recorded and used in accordance with agreed requirements, rules, and definitions to ensure integrity and consistency

### 3. Reliability

- Data collection processes must be clearly defined and stable to ensure consistency over time, so that data accurately and reliably reflect any changes in performance

### 4. 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

### 5. 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

### 6. Completeness

- Data should be complete
- Data should not contain redundant records

This list is paraphrased from DAMA, DMBOK, 2nd edition, 2017, 13.1.3.3, Table 29.



## 17. Appendix 2 - Data principles

| ID                                               | Name                                                       | Description                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enterprise data principles</b>                |                                                            |                                                                                                                                                                                                                                                                                                                                                         |
| 1                                                | Data are an asset                                          | Data have value to the University and are managed accordingly                                                                                                                                                                                                                                                                                           |
| 2                                                | Data are shared                                            | Users have access to the data necessary to perform their roles and responsibilities; therefore, data are shared across University functions and departments                                                                                                                                                                                             |
| 3                                                | Data are accessible                                        | Data are accessible for users to perform their functions                                                                                                                                                                                                                                                                                                |
| 4                                                | Data are quality assured                                   | Each data element has at least one recognised role accountable for data quality                                                                                                                                                                                                                                                                         |
| 5                                                | Data are protected                                         | Data are secured from accidental or malicious access (or alteration) by unauthorised users, whether in transit, at rest or in storage; and data are made available for legitimate need through authorised processes                                                                                                                                     |
| 6                                                | Data are reused                                            | Data are more valuable if they can be reused or used for more than one purpose. NOTE: The reuse of personal data, as defined by the Data Protection Act 2018, for a secondary purpose which is incompatible with the purpose for which data were originally collected, is unlawful.                                                                     |
| 7                                                | Data are defined by a common vocabulary                    | Data are defined consistently throughout the University, and definitions are understandable and appropriately published                                                                                                                                                                                                                                 |
| 8                                                | All data elements have an owner                            | Every data element has a named owner and ownership persists regardless of the use of that data                                                                                                                                                                                                                                                          |
| 9                                                | All data elements have a master (a Single Source of Truth) | Every data element has a single, known source (a Master data source) rather than multiple (potentially inconsistent) sources of the truth                                                                                                                                                                                                               |
| <b>Data governance and management principles</b> |                                                            |                                                                                                                                                                                                                                                                                                                                                         |
| 10                                               | Data governance is everyone's responsibility               | All data stakeholders contribute to data governance policies and their implementation and adoption                                                                                                                                                                                                                                                      |
| 11                                               | Data integrity is maintained                               | Any use of data is lawful across all decisions taken about the data                                                                                                                                                                                                                                                                                     |
| 12                                               | Data use is transparent                                    | Whenever possible, all parties using data or whose data are being used will know how they are being used. NOTE: In data protection terms there is an exemption for management forecasting and planning, which allows for any subject access requests or privacy notices surrounding that activity (for example, planning for a merger) to be suspended. |
| 13                                               | Data are standardised                                      | Specific guidelines and rules (including data definitions, availability, and privacy arrangements) are followed to ensure data are standardised                                                                                                                                                                                                         |
| 14                                               | Data are audited                                           | All data are open to audits and all decisions, controls, and processes about data can be subject to audits                                                                                                                                                                                                                                              |
| 15                                               | Data are managed by trained staff                          | Staff with responsibility for, and access to, data are appropriately trained and know where their responsibility for data lies including how to process or format data, and what to do in the event of a breach                                                                                                                                         |
| 16                                               | Data use is maximised                                      | Data are usable by anyone who needs them within authorised and lawful limits to optimise impact                                                                                                                                                                                                                                                         |

|    |                     |                                                                                                                                                                             |
|----|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17 | Data are controlled | Control procedures are in place to preserve the integrity of data (or data elements within records) and are used for the creation, storage, validation, updating, archiving |
|----|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|    |                                                                                     |                                                                                                                                                                                                                                                                                               |
|----|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                                                                     | and destruction of data (or data elements within records). NOTE: Control procedures, in so far as they relate to data elements of records, are aligned with University retention schedules.                                                                                                   |
| 18 | Data are assigned a lifecycle status                                                | All data elements have a lifecycle status assigned to identify if the data element is active or obsolete/inactive within lawful limits                                                                                                                                                        |
| 19 | Obsolete/inactive data are archived or destroyed                                    | Obsolete data are archived or destroyed following audit/compliance policies                                                                                                                                                                                                                   |
| 20 | Bulk data transfers are conducted only through a managed file transfer              | Bulk data transfers between applications are only undertaken through a managed file transfer method                                                                                                                                                                                           |
| 21 | Data transfers between applications are governed by data delivery agreements (DDAs) | Data Delivery Agreements (DDAs) are used as binding contracts between the source and target systems for any kind of data transfer between applications<br><br>Data transfers from the University to external parties must be managed and as appropriate be subject to controls and approvals. |
| 22 | Data are distributed/published only through managed interfaces                      | Managed interfaces are used to distribute or publish data and direct access to data tables is restricted                                                                                                                                                                                      |
| 23 | Data quality rules are managed as configurable data                                 | Data quality rules are not hard coded into the code of the application, instead a configuration driven data quality management tool manages the rules and their versioning                                                                                                                    |
| 24 | Sensitive data are identified, classified as confidential and protected             | Data identified as sensitive are protected and classified as confidential in line with the University's information classification policy of four tiers: Strictly confidential, Confidential, Internal and Public                                                                             |
| 25 | Data lineage is recorded and available                                              | Data lineage provides important metadata for data consumers and should be recorded and available where needed                                                                                                                                                                                 |

## 18. Appendix 3 - Roles and responsibilities of the data stewardship community

The data stewardship community comprises all staff who interact with data as part of their role at the University. Every member of staff has a role to play in the improvement of data quality; however, certain University officers have ownership or stewardship responsibilities for the active governance and management of data.

### Data owners

Data owners have responsibility for ensuring data are maintained to agreed quality standards.

Accountability: In line with University principles and guidelines data owner(s) are responsible for data management and governance activities in their data domain(s).

In line with University requirements the data owner will:

- Champion institutional compliance with the data governance policy
- Promote good data governance and data literacy in their business area
- Ensure consistency of approach in data collection, definition and sharing processes
- Maintain the principle of using 'golden source' data wherever reasonably possible
- Support data profiling activities in support of University strategies and initiatives
- Maintain relevant entries in institutional data dictionaries and local business glossaries
- Assign classifications to data items depending on their sensitivity based on the University Information Classification policy
- Authorise user access requests to golden source data where there is legitimate need
- Monitor data quality in line with approved and published dimensions
- Support data stewards to analyse data quality issues and identify and fix root causes of poor data quality
- Propose and manage data quality improvement activities
- Define and monitor data quality metrics
- Mandate changes to business processes and applications to improve data quality
- Propose new standards to improve data quality
- Escalate to the DGO if data quality issues cannot be resolved within a single domain
- Ensure the DGO has an accurate record of data stewardship assignments

### Data stewards

Data stewards are caretakers of systems data and are responsible for various day-to-day processes to ensure data fulfil business requirements including the understanding of current and downstream use of data for public information.

Accountability: In line with University principles and guidelines data stewards are accountable for local data usage in their data domain(s).

In line with University requirements the data steward will:

- Serve as a first point of contact for colleagues with data domain queries
- Train and coach system(s) users to understand and use data effectively
- Analyse data quality issues and propose improvements and/or solutions to data owners to eliminate root causes of poor data quality
- Follow agreed data management processes to manage data quality
- Support data owners to define and measure data quality metrics

- Manage approval processes for the use of domain data
- Adhere to the University Information Classification policy when using or providing data
- Propose new or amended data structures based on requirements for developments and initiatives
- Support the creation of conceptual data models and mappings
- Propose new standards to improve data quality
- Escalate to data owners if data quality issues cannot be locally resolved
- Support collaborative data governance and data literacy initiatives
- Provide the central point of communication for DAMG-related business

## Data consumers

Data consumers have responsibilities to participate in activities that define data for use.

Accountability: Data consumers are accountable for the proper usage of data as defined in Data Sharing Agreements.

In line with University requirements data consumers will:

- Participate in defining business terms and definitions to ensure usability within their business processes
- Participate in the identification of business rules, data quality rules, and data quality thresholds
- Participate in defining Data Sharing Agreements so they understand the authoritative source of data and any data constraints, such as security and privacy, for data usage
- Participate in the resolution of data issues as requested by data owners or their delegates
- Consume data only from authoritative sources identified by the DGO
- Identify data needs that are not supported by authoritative sources
- Identify data issues and bring them to the attention of data owners and/or their data stewards as soon as they are recognised
- Identify data control requirements that should be implemented by data owners to ensure quality and integrity in the data supply chain based upon the compliance requirements of the business processes

## 19. Appendix 4 - Responsibilities of the Data Governance Operations Group

The data stewardship community is supported by the framework elements identified in this policy including the Data Governance Operations Group (DGOps). The DGOps Group, led by the Head of Data Governance, co-ordinates and facilitates corporate data improvement activities and issue resolution.

**Accountability:** The DGOps Group has overall accountability for monitoring, maintaining and enhancing the University's data capability with specific responsibilities for corporate data held in the Data Warehouse.

The Group will:

- Ensure institutional alignment with the Data Governance Policy.
- Champion good data governance and data literacy across the institution.
- Ensure data-related roles and responsibilities are understood and adopted across the institution.
- Ensure master and reference data are sourced from agreed golden source(s) and available for institutional use.
- Oversee and co-ordinate, in collaboration with accountable data owners and data stewards, changes to data structures at source system level, which will impact on institutional data assets, system integrations and statutory reporting requirements.
- Curate central reference data (to be held within the Data Warehouse) to ensure institutional alignment and alignment within systems, for example, the University's organisational hierarchy.
- Manage data change request processes in relation to the Data Warehouse.
- Govern appropriate access to data in the Data Warehouse, in alignment with relevant policy and legislation.
- Co-ordinate sign off for data access requests, aligned with role-based access principles.
- Establish principles to monitor corporate data quality in the Data Warehouse in line with characteristics outlined in the Data Governance Policy.
- Plan the delivery of related training requirements.
- Manage the publication of the role-based data community matrix and maintain data stewardship assignments.
- Maintain and periodically review and recommend changes to

Data Governance Policy and underpinning standards, guidelines, and procedures.

- Ensure all data items are classified depending on their sensitivity based on the University Information Classification policy.
- In collaboration with accountable data owners and stewards, ensure that relevant corporate data are of the structure and granularity required for use in operations, reporting, decision making and planning.
- Ensure that end user documentation allows meaningful and consistent use and interpretation of source data.
- Support the procurement of new data source systems via outlining requirements to support alignment with the Data Governance Policy.
- Support the Business Design Authority with activities defined by the University’s strategic plans.

## 20. Version Control

| <b>Version number</b> | <b>Purpose / changes</b>                                                                                                          | <b>Document status</b> | <b>Author of changes, role and school / unit</b> | <b>Date</b>      |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------|------------------|
| 1.0                   | For consideration as a new IMEDA programme output                                                                                 | Approved               | IMEDA Programme Board                            | 11 December 2020 |
| 2.0                   | Incorporating minor changes following SDG meeting                                                                                 | Approved               | Principal’s Office                               | 16 June 2021     |
| 3.0                   | Incorporating minor improvements and historic changes relating to research data and defining the Head of Unit role as Data Owner. | Approved               | Head of Data Governance                          | 24 February 2025 |