Policy name	Data Governance and Quality Policy
Subject	Data Governance. Data Quality.
Approving authority	IMSSC
Accountable person	Chief Business Intelligence Officer
Responsible Team	Data Governance Team
First approved	December 2023
Version number	V 1.0

1   Introductory Purpose & Background

Data Governance provides robust data foundations on which the University can build its data capabilities to generate value, reduce costs and enable innovation.

Data Governance enables the University to understand the data we have and to identify which is the most important data. Data Governance establishes responsibilities, methods and processes to standardise as well as store and protect corporate data. It is different to Data Protection which relates to the lawful and fair use of personal data, though collaborative working between the two areas is essential particularly in relation to data sharing and information risks. A successful Data Governance capability enables the University to formalise the collection, management, and use of corporate data throughout its lifecycle.

Data Governance is a critical function in improving data maturity at the University that will benefit how data is processed and controlled at all levels and areas and in-line with institutional objectives.

Data maturity is essential to the University being able to monitor and realise its strategic objectives. Missing, incomplete or inaccurate data can present regulatory, reputational and financial risk. It is a condition of our registration with Office for Students (OfS) to provide and publish information as requested. You can find out more about OfS at the following link: https://www.officeforstudents.org.uk/.As part of this obligation, we are required to send a range of data to the Higher Education Statistics Agency (HESA) which is used to inform Higher Education regulation and policy and is also published as key performance metrics such as league tables. You can find out more about HESA at the following link: https://www.hesa.ac.uk/. Incomplete or inaccurate data can result in audit, financial penalty or a failure to meet our statutory obligations as a HE provider. Incomplete or inaccurate data also increases the risk of data breaches which pose both a significant regulatory and financial risk to the University.

2   Scope

The Data Governance and Quality Policy applies to any corporate data-related activities that are undertaken by staff (including contractual staff) across the University of Nottingham UK.

3   Definitions

Data

In the context of this policy, the term 'data' refers to corporate data. Corporate data is data that is owned, stored, processed and shared by the University of Nottingham UK.

Information

Information is created when data is processed, organised or structured to provide context or meaning.

Data Domain

A data domain is a logical grouping of data according to its identity and use across the University. For example, you may have a student data domain or a staff data domain.

Data Protection Legislation

The General Data Protection Regulation 2016 as enacted within the UK (UK GDPR) and Data Protection Act 2018 (DPA) as updated and re-enacted from time to time.

Data Quality

Data quality is the process of conditioning data to meet the specific needs of the University users and our beneficiaries.

Personal Data

Information relating to an individual, who can be identified directly or indirectly from that information. Personal Data can be factual (such as name, email address) or an opinion relating to that individual.

4   Policy

4.1 Key principles

In formalising the collection, management and use of data, data governance ensures that we maximise the use of data as a University asset. In defining a clear framework of data roles and responsibilities, data governance ensures that data is effectively owned and governed by data domain owners.

The University of Nottingham Data Strategy defines a series of core data principles to which the University is committed. It is important to note that these are distinct from the Data Protection principles. Further information in relation to the data protection principles can be found here:

https://uniofnottm.sharepoint.com/sites/InformationSecurityandCompliance

The University of Nottingham is committed to the following overarching data principle which drives all of our data-related activities:

Data is a valuable University asset

There are eight additional data principles that should be applied across all of our organisational activities:

Data is owned and governed
Data is fit for purpose
Data and information are business driven
Data is standardised, linkable and comparable
Data and information are secure
Data and information are appropriately accessible, available and reusable
Data issues are addressed strategically and systematically
People are supported to make good use of data

4.2 Key roles, responsibilities and/or requirements

Data Domain Owners are Executive level leaders with overall oversight of and accountability for the quality of one or more data sets.

Data Owners are Director level leaders responsible for the quality of data, steering and prioritising data governance activities and managing Data Stewards.

Data Stewards are Head/Manager level leaders appointed by the Data Owner to fulfil day to day data governance activities.

Data Quality and Standards Group will assist in driving and embedding the data governance operating model at the University of Nottingham by providing visibility of statutory data across the data domains and being a forum for developing and implementing data governance processes across the statutory data domains. The forum will be attended by relevant data domain owners and stewards from across the University.

IMSSC will receive updates from the Data Quality and Standards Group and will act as a point of escalation when required.

Head of Data Governance manages the operation of the 4 themes described in 4.3.

The assigned data governance roles for the University of Nottingham are shown below and can also be found on the Data Governance SharePoint site (internal access only).

Data Domain	Data Owner	Data Steward	Notes
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Reporting, data & Service Support	DIT / External Reporting and Systems / Fees and Funding
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Placements, mobility, partners & Visas	Global Engagement
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Programmes (Registration, enrolment & Engagement)	Programmes
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Assessments	Assessment
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Post-Graduate Research	PGR
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director Disability Services	Disability
Curriculum	Director of Registry and Academic Affairs	Deputy Director of Registry and Academic Affairs	Timetabling
Applicant	Director of Student Recruitment	Head of Admissions (UCAS/ITT)	UCAS
Applicant	Director of Student Recruitment	Head of Admissions (Direct)	Direct
Staff	Director of Human Resources	Associate Director of Hr Digital and Shared Services	Core HR Transactional Data, Organisational Hierarchy Data
Staff	Director of Human Resources	Digital Core – HR Data Lead	Core HR Transactional Data, Organisational Hierarchy Data
Staff	Director of Human Resources	Associate Director of Learning & Development	Learning and Professional Development People
Staff	Director of Human Resources	Digital Core Hr Subject Matter Expert	Learning and Professional

			Development People
Finance	Financial Controller	Head of Operations (Finance)	
Finance	Financial Controller	Head of Finance (Corporate)	
Planning and Performance	Director of Planning, Performance and Strategic Change	Associate Director for Statutory Returns and Data Governance	Statutory Reporting
Planning and Performance	Director of Planning, Performance and Strategic Change	Associate Director of Insight and Analysis	Analytics
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director Customer Service	Customer Service
Curriculum	Director of Registry and Academic Affairs	Head of Curriculum, Head of Student Records and Faculty Lead	Curriculum
Student (Sub-Domain)	Director of Registry and Academic Affairs	Associate Director - Assessments	Assessment

4.3.1 The Data Governance Operating Model

The Data Governance Operating Model is made up of two components: design and operation. The operating model design sets out the scope of data governance, allocating roles and responsibilities to staff identified as either critical stakeholders, data generators and consumers, partners and/or data experts. The design is the anchor for all operational activities. The operation component relates to how data governance is enabled and enacted on a day-to-day basis and relates to engagement and management activities as well as key partnerships.

The Data Governance Operating Model target state is outlined in the diagram below:
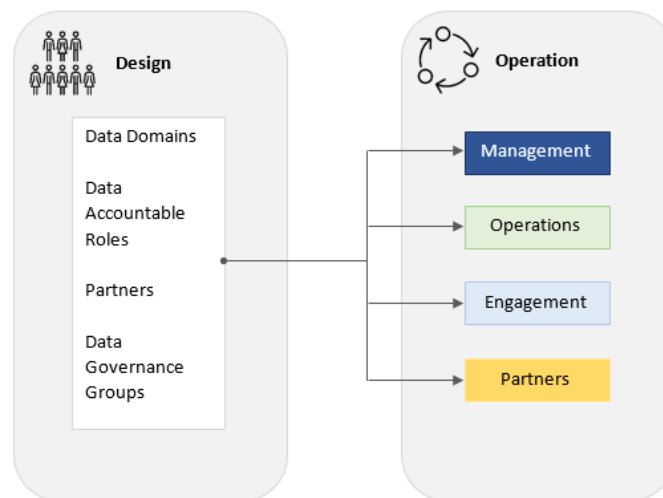
The operating model is underpinned by the four key themes outlined in the diagram below:

Management	Operation	Engagement	Partners
Working with and mentoring data domain roles. Ensuring responsibilities of roles are being met and managing some of the groups and boards.	Managing and maintaining the daily operation of the framework, with focus on data quality and business glossary. Includes how the framework supports new projects and initiatives.	Communicating with the institution on how to manage data as an asset. Supported by more focussed engagement for data governance roles and aligning with existing boards and groups.	Building and managing relationships with the key allies e.g., IT security, data protection, project management office, data architecture.

4.3.2 Data Quality

Data Quality is an important pillar of the Data Governance Framework. Whilst it operates in parallel to Data Governance, Data Quality is critical to maximising the use of data as a University asset.

In addressing data quality issues, there is an expectation that the root cause of poor data quality is understood and drives the subsequent response to fixing this. A principle of 'fix once' should always be applied, with data issues fixed once and at point of entry, to prevent a recurrence of poor-quality data.

There are a number of additional aims and objectives that the University of Nottingham has specifically in relation to data quality:

Aim	Supporting Objectives
Data is standardised, linkable and comparable	Standard methods are used to record individual data items across the University purposes and across systems, with clear ownership and process ensuring maximum reuse and sustainability.
Data issues are addressed strategically and systematically	Priority is given to addressing strategic root causes to enable lasting and effective solutions to be developed.
	Data quality metrics relating to material data should be proactively monitored and addressed, with data owners held accountable. Root cause analysis should be a central part of this, ensuring that data completeness and accuracy at the point of entry remains the common goal.
	Data duplication is avoided except where required due to specific technical or business constraints.
	A data forum which actively monitors and executes actions relating to external returns, data quality and data governance and which is attended by data stewards from across the University should be established and embedded.
People are supported to make good use of data	Training to enhance data literacy is routinely provided and refreshed, as part of the core training offer to staff across the University.

4.4 The consequences of non-compliance.

A lack of effective data governance can lead to widespread lack of trust in data, can pose reputational and regulatory risk, can mean that the University is unable to accurately identify, monitor and describe its positioning and performance, can lead to the duplication of data and can result in a duplication of effort.

There is no systematic triage and resolution mechanisms across the University to resolve issues found as close to source as possible. Missing, incomplete or inaccurate data can present regulatory, reputational and financial risk. It is a condition of our registration with Office for Students (OfS) to provide and publish information as requested. Incomplete or inaccurate data can result in audit, financial penalty or a failure to meet our statutory obligations as a HE provider. Incomplete or inaccurate data also increases the risk of data breaches which pose both a significant regulatory and financial risk to the University.

4.5 How compliance with the policy will be measured.

Compliance with the Data Governance and Quality Policy will be monitored by the Data Quality and Standards Group (DQSG). It is expected that data stewards and data owners will promote and drive compliance with the Data Governance and Quality Policy within their individual areas, with progress measured against the data governance measures log. The Data Governance Team will provide support and guidance in relation to the policy, ensuring that the aims and objectives of the policy are upheld and embedded.

4.6 Provisions for monitoring and reporting related to the policy.

The Data Quality and Standards Group (DQSG) will report into the Information Management and Security Steering Committee (IMSSC). The principal objective of the DQSG is to improve and develop the key University processes and reporting which rely upon data. The Group will meet bi-monthly with an agenda and actions that are driven by an emphasis on enhancing data quality through effective governance, accountability and collaborative working. The forum should uphold and promote the key principles of the Data Governance and Quality policy.

5   Review
As a minimum, this policy will be reviewed every two years.

6   Related policies, procedures, standards and guidance

Data protection - https://www.nottingham.ac.uk/governance/records-and-information-management/data-protection/data-protection-policy.aspx

Restricted Data Handling Policy – University Data Handling Policy 1.0 (2).pdf (Internal access only).

End of Document