DCU

Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Data Governance

Policy

Table of Contents

Introduction

DCU's institutional data are a valuable institutional resource that underpin and progress critical operational processes and provide critical information to support the university's mission and strategy. Data governance establishes responsibilities, processes, and guidelines to protect institutional data with a view to enhancing operational effectiveness, reducing risk, and supporting decision-making and reporting in the university. This policy reflects the university's commitment to strong data governance and data management, which will underpin a strategic commitment to organisational effectiveness and intelligence-enabled decision making.

In implementing this policy, the university seeks to maximise the value of its data while minimising risks associated with data misuse or mismanagement. All members of the university community are encouraged to engage with this policy and contribute to the responsible management of institutional data. While the principles of data governance extend to all data systems in the University, the initial phase of implementation will focus on data held on core university systems. The systems holding these categories of data can be referred to as "Data Domains".

Purpose

The policy aims to:

- Define the scope, purpose, and vision for data governance at DCU;
- Outline a DCU Data Governance Framework and associated responsibilities for the development and implementation of data governance at DCU;
- Identify and define key roles and responsibilities for the management of institutional data at DCU; &
- Provide clarity on key data governance terminology and concepts.

Scope

The implementation of data governance focuses on data held for the purposes of managing the university as an organisation and therefore excludes data generated, stored, and used for the purposes of scholarship by both students and staff.

This policy applies to all university staff and is particularly relevant to colleagues who handle and manage organisational data as part of their role.

Definitions

Data governance at DCU is defined as the active and ongoing development of institutional capability through the coordination of people, processes, and technology to manage institutional data as a critical university resource. Data governance is underpinned by robust policies, guidelines, and practices that ensure data is protected, managed, and used responsibly and effectively throughout the data lifecycle.

See the Appendix to this policy for a glossary of Data Governance Terms.

Policy Statement

Principles Underpinning Data Governance at DCU

Data Governance policy and practice are **Clear**	Data governance policies, guidelines, and practice are clear and transparent. Access to, and the use of institutional data have clear lines of responsibility and accountability and shall be approved through defined and transparent access approval procedures.
Institutional Data at DCU are **Managed**	Institutional data shall be actively verified, managed, and curated throughout its lifecycle. Staff with responsibility for, and access to, institutional data are appropriately trained and are knowledgeable on their responsibilities for the appropriate management of data in line with their role's responsibilities.
Institutional Data at DCU are **Protected**	Institutional data are protected from accidental, malicious, or unauthorised access, misuse, or alteration. Data governance balances robust access procedures with making necessary data and information accessible and usable for legitimate organisational purposes.
Institutional Data at DCU will be **Consistent**	Data governance supports consistent standards for managing and overseeing institutional data across functions and systems. Data are defined consistently throughout the University where possible, and definitions are understandable and appropriately shared internally.
Institutional Data at DCU are **Trustworthy**	Data management shall ensure accurate, well-defined, and trustworthy data that can be reliably used to fulfil crucial business processes and interpreted to inform decision-making and planning.
Data Governance is implemented through **Partnership**	Data governance and the management of data quality will be a collective responsibility. Colleagues will have the opportunity to contribute to the development of data governance policies and will work together on their implementation and adoption.

Expected Impact of Data Governance

Improved Clarity

The implementation of data governance will improve clarity on roles and responsibilities in relation to data and ensure colleagues have a shared understanding of institutional data, its purpose, and how it is being used.

Operational Efficiencies

The implementation of data governance and data management practices shall contribute to organisational efficiencies by improving data accuracy, consistency, and completeness. Reliable and well organised data will improve operational efficiencies and empower better, faster, and more informed decision-making.

Improved Knowledge and Awareness

The implementation of data governance will support enhanced organisational knowledge on good data management practices and heightened awareness on how data are used across the university.

Enhanced Utilisation of Data

The implementation of data governance will reinforce good practice in data management and data quality resulting in data that can be more widely used to inform decision-making through enhanced management reporting.

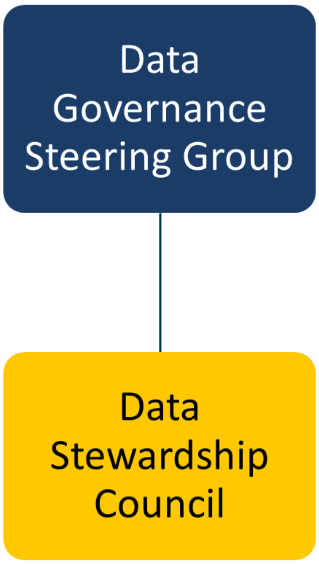
Reduced Risk

The implementation of the Data Governance Framework at DCU will align with and contribute to existing data privacy and security compliance and practice to protect data as a critical university resource.

A Framework for Data Governance

The Data Governance Policy establishes a framework for the responsible oversight, accessibility, and protection of institutional data. It is designed to promote consistency, accountability, and collaboration across all functions of the university, ensuring that data is managed as a shared resource that benefits the entire university community.

Institutional level oversight for the implementation of data governance shall be driven by two university level committees, both with distinct remits and responsibilities. At a strategic level, the Data Governance Steering Group develops and approves data governance policies and approaches, ensuring their alignment with the strategic priorities of the university. The Data Stewardship Council focuses on the cross institutional implementation of policy and good practice in data governance and data management.



Data Governance Steering Group

- Executive leadership and oversight of the implementation of Data Governance and DCU.
- Development and approval of policy, guidelines, and monitoring implementation of Data Governance initiatives
- Ensuring alignment of Data Governance to DCU Strategy, IS Governance and other institutional strategies

Data Stewardship Council

- Support operationalisation of data governance.
- Develop and implement tools and protocols for data quality management
- Share good practice and data governance challenges
- Identify data governance capacity building requirements
- Make recommendations to Steering Group on further development of Data Governance Framework

Roles and Responsibilities

The roles and responsibilities of staff engaging with this policy are as follows:

Data Owner
DCU, as an institution, is the <u>owner</u> of all institutional data.

Data Trustee
Data trustees have ultimate responsibility for the overall oversight of data domains under their executive remit and may have responsibility for multiple data domains.

Data Trustees are responsible for:

- Overseeing the implementation of data governance policies, procedures and initiatives in areas under their executive leadership.
- Encouraging continuous improvement in how data are managed and used within their areas of responsibility.
- Having oversight of risks related to data misuse, loss, or inaccuracy in their areas of responsibility.
- Making decisions and assigning decision-making authority on how data within their domain is managed and shared.
- Working with other trustees, stewards, and relevant units to enable and support evidence-informed decision making and institutional reporting.

Data Stewards
Data stewards have responsibility for overseeing the implementation of data governance and data quality within their university department or unit. Data stewards are a source of institutional knowledge of data quality and data management issues within their department or unit.

Data stewards take a leadership role in ensuring that data governance is incorporated into practice within their area and are responsible for:

- Contributing to the development and implementation of data governance policies, procedures and initiatives in their department or unit.
- Encouraging strong data management approaches to handling institutional data.
- Working with colleagues to ensure Standard Operating Procedures (SOPs) include processes deliver consistency in how data is handled in the department or unit.
- Ensuring processes are in place to identify and resolve data quality issues in their department or unit.
- Ensuring processes are in place for data access control to protect sensitive data.
- Working with colleagues from other areas of the university on aligning data practice and meeting cross-institutional information needs.
- Overseeing the maintenance of data dictionaries and metadata repositories that describe the content, context, and structure of data assets.
- Maintaining knowledge on upstream and downstream dependencies for data in their Area.

Data Processors
Data processors are individuals who have responsibilities to create, handle, manage and process data on university systems as part of their roles. Data processors include colleagues working with system data daily, and those who less frequently create or input data onto university systems as a part of their role.

Data processors are responsible for:

- Exercising due care in creating and entering data on university systems.
- Using defined Standard Operating Procedures (SOPs) (where available) for handling institutional data to ensure the accurate and secure entry, processing, and maintenance of data.
- Ensuring that data is handled in accordance with university policies, including data privacy, data retention, data classification, and data security policies and in line with authorised purposes.
- Escalating recurrent issues with data quality to their line manager, where appropriate.
- Remaining knowledgeable on changes to SOPs, coding conventions, or rules relating to data entry on systems they input data into.
- Remaining informed about the implications of incomplete or inaccurate data to the university business processes and reporting capabilities.

Data Users
Data Users are individuals who access and use institutional data as part of their duties.

Data users are responsible for:

- Using institutional data solely for authorised academic, administrative, or research purposes. No institutional data should be used for research purposes in the absence of ethical approval, and access approval.
- Only accessing institutional data that is necessary in the conduct of their role, and for its authorised purpose.
- Treating DCU data as confidential and for internal use only.
- Following institutional security policies to protect data from unauthorised access, loss, or corruption.

- Staying informed about institutional data policies and participate with training and development opportunities, where possible.

Data Custodians

Data Custodians are responsible for managing and protecting institutional data to ensure its security, accuracy, and compliance with regulatory and institutional policies. Data custodians typically involves overseeing technical aspects of data storage, access, integration, and processing.

Data custodians are responsible for:

- Overseeing the implementation of user access permissions and access control on university systems.
- Overseeing the safe storage, archiving and disposal of institutional data on the systems for which they are responsible.
- Ensuring the appropriate handling of data migration and integrations on university systems.
- Advising on protection of university data from cyber security risks.

Related Documentation

This policy should be read in conjunction with the following policies:

- Data Privacy Policy
- Compliance Policy
- Personal Data Retention Policy
- Data Classification Policy
- Digital Access Control Policy
- Digital Identity Retention Policy
- Information & Communications Technology (ICT) Security Policy
- Personnel Files Access Policy

Contact

Any queries regarding this policy should be directed Aisling McKenna, Data Governance and Strategy Intelligence.

Policy Review

This policy will be reviewed every three years by the Data Governance Steering Group. Any substantial change to the Policy will be brought to the DCU Executive for approval.

Version Control

Document Name	Data Governance Policy		DCU Ollscoil Chathair Bhaile Átha Cliath Dublin City University
Unit Owner	Data Governance and Strategic Intelligence		
Version Reference	**Original - V1.0**	**Reviewed - N/a**	
Approved by	Executive	N/a	
Effective Date	April 1st 2025	N/a	

End.

Appendix: Data Governance Glossary of Terms

Term	**Explanation**
Access Management	The continual process of deciding, assigning, reviewing, and amending permissions to individuals and groups to ensure access to the organisations data, while maintaining data security.
Business Intelligence	The processes and technical infrastructure that collects, stores, and analyses organisational data for use in decision-making, evaluations and planning.
Business Process	The sequencing of decisions, tasks and activities to produce an output necessary for university operations.
Data	Numbers, texts, codes, or images that are owned, stored, processed and shared by the university. Initially data within the scope of DCU Data Governance policy relates to data held within core university systems.
Data Custodians	Identified individuals with responsibility for the technical or systems level data matters, including storage, access, security, integration, and automated data processing.
Data Dictionary	A database or source of information about data and database structures. A catalogue of all data elements, containing their names, structures, and information about their usage, for the benefit of programmers and others interested in the data elements and their usage.
Data Domain	A definable set of institutional data, typically from a single database or system, or several systems linked by ownership.
Data Governance	The active and ongoing development of institutional capability through the coordination of people, processes, and technology to manage institutional data as a critical university resource.

Term	Explanation
Data Governance Framework	The structure through which the university establishes responsibilities for the oversight of institutional data.
Data Integration	The process of bringing together data from multiple sources across the university to enable business processes or reporting capabilities.
Data management	Activities that control how data is generated, stored, checked, used, and disposed of data across the data lifecycle.
Data Privacy	Organisational controls to protect personal data, including how the university stores collect, store and use personal data. Data privacy is also used in this context to describe alignment of data practice to requirements under the General Data Protection Regulation (GDPR).
Data Processors	Data processors are staff who, as part of their job, undertake activities that generate, handle, or amend data on university systems.
Data quality	The extent to which institutional data meets requirements for accuracy, completeness, consistency, timeliness so that it fulfils the needs of the organisation.
Data Steward	An identified person or persons with responsibility for overseeing the implementation of data governance and data quality within their university department or unit.
Data Trustees	A senior leader with ultimate responsibility for the overall oversight of data domains within their area of executive responsibility.
Data Users	Individuals who access and use institutional data as part of their duties, but do not generate or amend the data on institutional systems.
Decision Rights	Rules and protocols making decisions on the “who, and when, and how, and under what circumstances” regarding institutional data access.
Metadata	A set of data that describes other institutional data. Metadata provides information about data within institutional systems. This may include its location, definitions, type of data, its source, coding parameters, etc.
Standard Operating Procedures	A set of defined step-by-step instructions for performing a routine activity. In the case of the university, standard operating procedures may relate to describing how business processes are conducted.

End.