Data Governance Policy

Policy Category:	Governance
Subject:	Data Governance
Approving Authority:	President & Principal
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	Business Assurance
Related Procedures:	Data Governance Procedure Data Protection Procedure Information Classification Procedures
Related College Policies:	Records Management Policy Data Protection Policy IT Acceptable Use Policy Research Data Management Policy
Effective Date:	July 2021
Supersedes:	April 2015
Last Review:	November 2024
Next Review:	July 2027

I. Purpose & Scope

1.1 This policy applies to all university processes where data is used or managed including but not limited to finance data, estates data, organisational structured data and network data as well as personal data as defined in the data protection policy.

1.2 This policy applies to everyone at the university and, particularly, any person involved in specifying data processes, accepting external data, or providing expert input, must be familiar with this Data Governance Policy.

II. Definitions

2.0 Table of Definitions

Data	Raw information and statistics collected for reference or analysis, including but not limited to machine readable data, data in print, backups, and archives.
Data Set	A collection of data that is used to analyse trends, help form business strategy and decisions.
Data Governance Committee	A committee made up of main stakeholders of College data, who will assist in resolving data related issues that arise and providing direction for strategy and policy for data.

Data Governance Manager	Main point of contact for data governance framework, policies, and standards while analysing issues in College data.
Data Steward	A senior member of the university responsible for one or more data sets.
Data Custodian	Data custodians are individuals who have operational level responsibility for the capture, maintenance, and storage of data.
Data User	Any individual or system that uses data for undertaking college business.
Data Enabler	A team or department which is not responsible for the data but facilitates the gathering, storage and retention of data belonging to another area of the university.
Information	What is conveyed or represented by a particular arrangement or sequence of things, such as data.
IT System	A place or platform where College data can be entered, stored, retrieved.

III. Policy

3.0 Principles of Data Governance

3.1 The principles below are in accordance with ISO 38505 and have been adopted by the university to govern institutional data.

Data are a valuable asset	Data are valuable to the university and needs to be managed efficiently and protected with clear ownership and management.
Data Transparency	The College will be transparent about the data that decisions are based on, and where possible proactively publish data.
Data Quality	Data collected and used by the College is to be reliable and accurate and complete. Data quality issues identified by any data user should be reported using the appropriate data quality issue process.
Data Accessibility	Data are shared with staff where it is necessary to perform their role, therefore one dataset may be required to be shared across different university functions in a timely manner. Personal data is shared in compliance with the Data Protection Policy.
Contextual Data Management	The use of data will have clear procedures and the context and rules of how the data is gathered and held will be documented.
Data Definitions	Data will be defined consistently throughout the university through a data dictionary and consistent terminology is to be used across the university.

4.0 Law, regulations and standards

4.1 Nothing in this policy precludes any steps that need to be taken to comply with the law to disclose information to external organisations or governmental agencies. The university will work to best practice standards for data governance.

5.0 Ownership and management of data

5.1 Institutional data is owned by the university, not by any individuals. A department may have delegated responsibility for some datasets. Data Stewards have ultimate responsibility to manage the data within their authority in compliance with the law and university policies.

5.2 All users of data have responsibility for preserving the security and integrity of university data. All data users must:

- treat the data in accordance with the College's information classification procedures;
- observe any ethical restrictions applied to the data;
- adhere to policies or procedures that apply to the data;
- ensure the quality of data and any analysis results they provide are accurate and interpreted correctly, free of bias;
- have proper access controls in place. Any breaches of access controls where personal data is shared inappropriately need to be reported as defined in the data breach management procedure.

5.3 This policy will be enforced by the Data Governance Committee, Data Stewards and Data Custodians.