Information Security Policy

Policy Category:	Governance
Subject:	Information Security Management
Approving Authority:	University Executive
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	Business Assurance
Related Procedures:	Data Governance Procedure Data Protection Procedure Information Classification Procedure Code of Connection Procedure
Related College Policies:	Records Management Policy Data Protection Policy Information Security Risk Management Policy IT Acceptable Use Policy
Effective Date:	9 March 2023
Supersedes:	None
Last Review:	N/A
Next Review:	2024

I. Purpose & Scope

1.1 The purpose of this policy is to ensure that information is appropriately secured to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

1.2 This policy applies to any individual who has access to the university's systems and services and anyone who uses or manages data in any format in the course of university business.

1.3 It addresses all information, regardless of the form or format, collectively termed 'Information Assets' which are created or used in support of business activities.

II. Definitions

Data is raw information and statistics collected for reference or analysis, including but not limited to machine readable data, data in print, backups, and archives.

The **Data Governance Committee** is a committee made up of the primary stakeholders of university data, who will assist in resolving data related issues that arise and provide direction for strategy and policy for data.

A **Data Steward** is a senior member of the university responsible for one or more data sets.

Data Custodians are individuals who have operational level responsibility for the capture, maintenance, and storage of data.

A **Data User** is any individual or system that uses data for undertaking university business.

Information is conveyed or represented by a particular arrangement or sequence of things, such as data.

Information Asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited efficiently. Information Assets have recognisable and manageable value, risk, content, and lifecycles.

Information Security is the preservation of Confidentiality (protecting information from unauthorised access and disclosure) Integrity (safeguarding the accuracy and completeness of information) and Availability (ensuring that information and associated services are available to authorised users when required)

Systems and Services are places or platforms where university data can be entered, stored, or retrieved.

III. Policy

3. Principles of Information Security

3.1 Information Security principles are aligned where practicable with ISO 27001:2018 to secure institutional data.
3.2 Information will be protected in line with all relevant university policies and legislation.
3.3 Information will be classified according to the university's Information Classification Procedures
3.4 The integrity of information will be maintained.
3.5 It is the responsibility of all individuals who have been granted access to information to handle it appropriately.
3.6 Information will be protected against unauthorised access.
3.7 Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the information and ensuring that appropriate security measures are in place to protect the information asset.
3.8 Information will be made available solely to those who have a legitimate need for access.

IV. Ownership and Management of Data

4.1 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.
4.2 All users of data have responsibility for preserving the security and integrity of university data. All data users must:

4.2.1 treat the data in accordance with the university's information classification procedures
4.2.2 observe any ethical restrictions applied to the data
4.2.3 adhere to policies or procedures that apply to the data
4.2.4 ensure the quality of data and any analysis results they provide are accurate and interpreted correctly, free of bias

4.2.5 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.

V. Enforcement

5.1 Any action which breaches the terms of the Information Security Policy, and its associated policies is an infringement of King's regulations and will be investigated and dealt with in accordance with the appropriate university regulations.

VI. Review and Continual Improvements

6.1 A review of this policy will be undertaken by the Business Assurance Team at a minimum biennially.