Data and Information Governance Policy

Section 1 - Background

(1) Institutional data and information are strategic assets of Australian Catholic University (ACU). Appropriate governance for the management and use of data and information is critical to the University's success. Inappropriate governance can result in breaches of legislation / regulations and inefficiencies and exposes the University to significant risks.

(2) Effective data and information governance can result in optimal leverage of data and information and provide the foundation for improved, data-driven decision-making and culture. A consistent, repeatable, and sustainable approach to data and information governance is necessary to protect the security and integrity of, and optimise the leverage of, the University's data assets.

Section 2 - Purpose

(3) The purpose of this Policy is to:

a. define the roles and responsibilities for data and information usage and establish clear lines of accountability;
b. develop best practices for effective data and information management, governance and protection as developed and determined through the ACU Data Strategy;
c. protect the University's data and information against internal and external threats (e.g. breach of copyright, privacy and confidentiality);
d. support data and information leverage and streamline data and information access and sharing to appropriate users to enable data-driven decision making;
e. ensure that the University complies with applicable laws, regulations, and standards; and
f. ensure that a data trail is effectively documented within the processes associated with creating, accessing, retrieving, reporting, managing and storing of data and information.

Section 3 - Scope

(4) This Policy applies to all institutional data and information used in the administration of the University and all of its Organisational Units, except data and information used for the purpose of academic research. This Policy covers, but is not limited to, institutional data and information in any form, including print, electronic, audio-visual, and backup and archived data. The Policy applies to all ACU staff, third parties, contractors and consultants. Data and information used for the purpose of academic research is governed under the Research Data Management Policy.

Section 4 - Principles

Strategic:	ACU is the owner of all institutional data and information and leverages its value as a strategic asset to support the University's mission, vision and strategic priorities, and as defined by the ACU Data Strategy.
Quality:	the quality and integrity of data and information must be upheld by data stewards, managers, developers and users. As far as practicable, every data source must have a Data Steward.
Accessible:	data and information must be findable, accessible and useful for University purposes, with appropriate authorisation and supported by clearly defined data and information classification standards.
Secure:	data and information must be captured, classified, stored, distributed and managed securely and appropriately and in accord with applicable University policies and procedures.
Reuse:	as a University asset, data and information must be available for reuse and interoperable wherever possible, through integrated, linking and data sharing to further expand the institutional value of information and data. Information and data must be used solely for its intended purpose(s).

Section 5 - Management and Use of Data

(5) Data and information will only be developed, collected and distributed for legitimate and appropriate uses that add value to the University. This requirement excludes employment-related information and data that is used by individual staff members for their respective job applications and online professional profiles (e.g. LinkedIn, Seek) and only if this information and data are solely of a general and non-sensitive nature.

(6) Extraction, manipulation and reporting of data and information must be done only to perform University business.

(7) Personal use of institutional data and information, including derived data and information, in any format and at any location, is prohibited.

(8) Appropriate approval (as defined in the Data and Information Governance Procedure) is required before any ACU owned data or information (that is not public) is shared outside the University.

(9) Data Stewards and their respective Data Managers must ensure the process for the administration of data is in accordance with the Data and Information Management Life Cycle (as per Section 7).

(10) Data records must be kept up to date throughout every stage of the workflow in an auditable and traceable manner. Data Stewards and their respective Data Managers are responsible for ensuring that a data trail is effectively documented within the processes associated with accessing, retrieving, reporting, managing and storing of data and information. When data is transferred from one Data Source to another, this responsibility is transferred to the Data Steward of the receiving Data Source.

(11) Data and information shall be retained and disposed of in an appropriate manner in accordance with the Records and Archive Management Policy and the Records Retention and Disposal Schedule. Retention Schedules can only be applied to ACU structured data that has been clearly named, classified and aligned with the agreed business classification scheme.

(12) Institutional data and information developed, distributed and / or used in projects shall fall under the same governance requirements as above, in that data roles for new and existing data, must be adhered to and implemented early as part of the solution development life cycle, not post-solution deployment.

(13) The definitions and terms used to describe different types of data and information will be defined consistently across the University. To enable this, the data classifications and definitions listed in the Data and Information Governance Procedure will be used and observed.

(14) Appropriate data quality and security measures (including those listed in the Data and Information Governance Procedure) must be adhered to at all times to assure the safety, quality and integrity of University data. Data privacy

will be maintained as determined in the Privacy Policy, specifically in respect to all data relating to personal information managed across ACU.

(15) Data and information stored in an electronic format must be protected by appropriate electronic safeguards and / or physical access controls that restrict access only to authorised user(s). Similarly, data and information in hard copy format must also be stored in a manner that will restrict access only to authorised users.

Section 6 - Roles and Responsibilities

Data Owner	ACU, rather than any individual or Organisational Unit, is the owner of all data.
Governing Authority	Responsible for overseeing the approval, implementation and communication of this Policy and the Data and Information Governance Procedure across ACU.
Data Trustee	Member of the Senior Executive* with planning and decision-making authority for institutional data. Data Trustees and through their nominated delegates are responsible for overseeing the continuous improvement of the University's data and information governance and management. *as listed in the Delegations of Authority Policy and Register - Management Levels 1 and 2
Data Steward	Member of the Executive** who oversees the capture, maintenance and dissemination of data within the remit of their designated role, functional area, or system administration. Data Stewards are responsible for assuring the requirements of this Policy and the Data and Information Governance Procedure are followed within their area of responsibility. **as listed in the Delegations of Authority Policy and Register - Management Level 3
Data Manager	Any member of staff with operational responsibilities in assisting Data Stewards or Trustees with day-to-day data administration activities; including, but not limited to developing, maintaining, distributing and securing institutional data. Data Managers are expected to have high-level knowledge and expertise in the content of data within their area of responsibility.
Data Developer	Any member of staff or authorised agent who accesses, inputs, amends, deletes, extracts, and analyses data to develop original reports, data sets and other outputs that are then distributed to data users. Data developers are responsible for the quality assurance of the data that they gather, compile and distribute.
Data User	Any member of staff or authorised agent who accesses, extracts, applies and analyses data in order to perform their day-to-day duties to develop reports, new data sets and other outputs. Data Users are not generally involved in the governance process but are responsible for the quality assurance of how they apply data to develop subsequent reports, new data sets and other outputs.

Section 7 - Data and Information Management Lifecycle

(16) All University data must be managed in accordance with the Data and Information Management Life Cycle and the Data and Information Governance Procedure.

Section 8 - Definitions and Terms

(17) To establish operational definitions and facilitate ease of reference, the following terms are defined:

Term	Definition
Access	The right to read, copy, edit or query data.

Term	Definition
Institutional Data and Information	All data or information developed and / or collected by the University in relation to its business activities in any form including print, electronic, audio-visual, backup and archive formats. It includes but is not limited to data and information that relates to students, staff, teaching and learning, research management, external engagement, web and social media, systems, finance, property and facilities but excludes “research data” as defined in the Research Data Management Policy.
Data and Information Management Life Cycle	The process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of the University.
Data Source / Source System	A provider, system, warehouse or platform that stores or publishes data or sets of data and information or provisions integration of data into other systems or data repositories.
Data Integrity	Refers to the accuracy and consistency of data over its entire life cycle.
Data Quality	Refers to the validity, relevancy and currency of data.
Information Security Incident	Any incident where the security on ACU information and data may have been or has been compromised or breached.
Security	Refers to the safety of University data in relation to the following criteria: access control; authentication; effective incident detection, reporting and solution; physical and virtual security; and change management and version control.

Section 9 - Review

(18) This Policy will be reviewed and updated every five (5) years from the approval date, or more frequently if appropriate. In this regard, any staff members who wish to make any comments about the Policy may forward their suggestions to the Responsible Officer.

Section 10 - Revisions made to this Policy

(19) This Policy has been revised as determined by consultation, research and development performed through the ACU Data Strategy. To access information about this work, please contact the Responsible Officer.

(20) Unless otherwise indicated, this Policy will still apply beyond the review date.

Section 11 - Further Assistance

(21) Any staff member who requires assistance in understanding this Policy should first consult their nominated supervisor who is responsible for the implementation and operation of these arrangements in their work area. Should further assistance be needed, the staff member should contact the Responsible Officer for clarification.

Status and Details

Status	Current
Effective Date	9th February 2024
Review Date	25th January 2026
Approval Authority	Vice-Chancellor and President
Approval Date	9th February 2024
Expiry Date	Not Applicable
Responsible Executive	Scott Jenkins Chief Financial Officer
Responsible Manager	Phil Avery National Manager, Planning and Analysis
Enquiries Contact	Financial Corporate Services