Name of Policy	Data Governance Policy
Description of Policy	To establish proper standards to assure the quality and integrity of University data. This policy also defines the roles and responsibilities of University staff and its agents in relation to data access, retrieval, storage, destruction, and backup to ensure proper management and protection of data is maintained.
Policy applies to	☒ University-wide ☐ Specific (*outline location, campus, organisational unit etc.)* _____
	☒ Staff Only ☐ Students Only ☐ Staff and Students
Policy Status	☒ New Policy ☐ Revision of Existing Policy
Description of Revision	

Approval Authority	Vice-Chancellor
Governing Authority	Information Communication Technology Advisory Committee (ICTAC)
Responsible Officer	Director, Office of Planning and Strategic Management

Approval Date	3 March 2014
Effective Date	3 March 2014
Date of Last Revision	n/a
Date of Policy Review*	3 March 2019

** Unless otherwise indicated, this policy will still apply beyond the review date.*

Related Policies, Procedures, Guidelines and Local Protocols	Acceptable Use of IT Policy Code of Conduct for All Staff Communication Policy Computer Use Policy Copyright and Moral Rights Data Classification Policy and Procedure (to be developed) Data Governance Procedures (to be developed) Intellectual Property Policy Policy on Policy Development Records and Archives Policy Records Retention and Disposal Schedule Telecommunications Usage Policy

Table of Contents

1 BACKGROUND INFORMATION

Institutional data is a strategic asset of Australian Catholic University (ACU) and the appropriate governance for management and use of data is critical to the University's operations. Inappropriate governance can result in inefficiencies and exposes the University to unwanted risk. A consistent, repeatable, and sustainable approach to data governance is therefore necessary in order to protect the security and integrity of the University's data assets.

2 POLICY PURPOSE

The purpose of the Data Governance Policy is to:

- Define the roles and responsibilities for different data usage and establish clear lines of accountability;
- Develop best practices for effective data management and protection;
- Protect the University's data against internal and external threats (e.g. breach of privacy and confidentiality);
- Ensure that the University complies with applicable laws, regulations, and standards; and
- Ensure that a data trail is effectively documented within the processes associated with accessing, retrieving, reporting, managing and storing of data.

3 POLICY SCOPE

This policy applies to all institutional data used in the administration of the University and all of its Organisational Units, except data used for the purpose of academic research. This policy covers, but is not limited to, institutional data in any form, including print, electronic, audio-visual, and backup and archived data.

4 DEFINITION AND TERMS

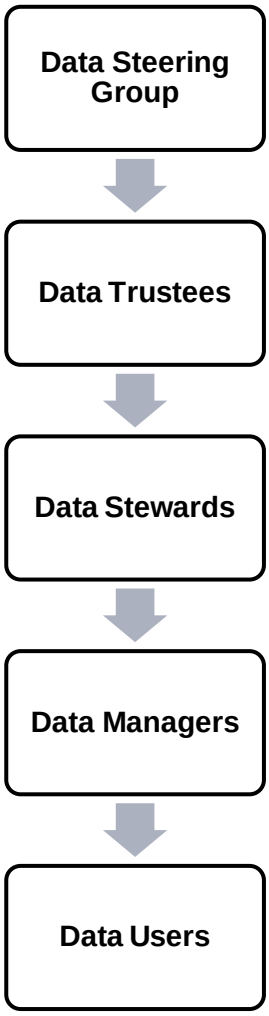
To establish operational definitions and facilitate ease of reference, the following terms are defined:

Access – the right to read, copy, or query data.

Data or Institutional Data – a general term used to refer to University's information resources and administrative records which can generally be assigned to one of four categories:

- Public access data – data that is openly available to all staff, students, and the general public.
- Internal general data – data used for University administration activities and not for external distribution unless otherwise authorised.
- Internal protected data – data that is only available to staff with the required access in order to perform their assigned duties.
- Internal restricted data – data that is of a sensitive or confidential nature and is restricted from general distribution. Special authorisation must be approved before access or limited access is granted.

Data Governance Hierarchy – outlines the access rights, roles and responsibilities of ACU staff in relation to the management and protection of data:



Information Communication Technology Advisory Committee or ICTAC– is a University wide committee, with members consisting of Data Trustees, Data Stewards and designated Data Users. ICTAC is responsible for approving the procedures related to the Data Governance Policy. ICTAC also assures appropriate data processes are used in all of the University's data-driven decisions.

Data Trustee – is a Member of the Senior Executive Group with planning and decision-making authorities for ACU's institutional data. The Data Trustees, as a group, are responsible for overseeing the continuous improvement of the University's data governance and management.

Data Steward – is a Member of the Executive who oversees the capture, maintenance and dissemination of data for a particular Organisational Unit. Data Stewards are responsible for assuring the requirements of the Data Governance Policy and the Data Governance Procedures are followed within their Organisational Unit.

Data Manager – has operational responsibilities in assisting Data Stewards with day-to-day data administration activities; including, but is not limited to: develop, maintain, distribute, and secure institutional data. Data Managers are expected to have high level knowledge and expertise in the content of data within their responsible area.

Data User – is any staff or authorised agent who accesses, inputs, amends, deletes, extracts, and analyses data in order to carry out their day-to-day duties. Data Users are not generally involved in the governance process, but are responsible for the quality assurance of data.

Data Management Life Cycle – refers to the process for planning, creating, managing, storing, implementing, protecting, improving and disposing of all institutional data of the University (see Appendix 1).

Integrity or data integrity – refers to the accuracy and consistency of data over its entire life-cycle.

Member of the Executive – is defined as the positions which normally report to either the Vice-Chancellor or a Member of the Senior Executive, and having staffing and supervisory responsibilities.

Quality or data quality – refers to the validity, relevancy and currency of data.

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.

Senior Executive Group or SEG –is the peak senior strategic forum of ACU. The SEG is chaired by the Vice-Chancellor with members consisting of the Provost/ Deputy Vice-Chancellor (Academic); Chief Operating Officer/ Deputy Vice-Chancellor; Deputy Vice-Chancellor (Research); and Deputy Vice-Chancellor (Students, Learning & Teaching).

5 POLICY PRINCIPLES

The following principles outline the minimum standards that guide the University's data governance procedures and must be adhered to by all ACU staff:

5.1 ACU, rather than any individual or Organisational Unit, is the owner of all data. A Data Trustee has the responsibility for the management of data assigned within their portfolio. A Data Steering Group, in the form of the Information Communication Technology Advisory Committee is responsible for the overall management of the University's data governance.

5.2 Every data source must have a Data Steward who is responsible for the quality and integrity, implementation and enforcement of data management within their Organisational Unit. Data Managers are responsible for ensuring effective local protocols are in place to guide the appropriate use of data.

5.3 Access to, and use of, institutional data will generally be administered by the appropriate Data Manager.

5.4 The Data Steward, having determined the category of the institutional data as confidential, will approve access based on appropriateness of the User's role and the intended use. Where necessary, approval from the Data Trustee may be required prior to authorisation of access.

5.5 Data Manager must ensure the process for the administration of data is in accordance with the Data Management Life Cycle (See Appendix 1).

5.6 Data Users must ensure appropriate procedures are followed to uphold the quality and integrity of the data they access.

5.7 Data records must be kept up-to-date throughout every stage of the workflow and in an auditable and traceable manner.

5.8 Data should only be collected for legitimate uses and to add value to the University.

5.9 Extraction, manipulation and reporting of data must be done only to perform University business:

a. Personal use of institutional data, including derived data, in any format and at any location, is prohibited.
b. Where appropriate, before any data (other than publically available data) is used or shared outside the University, verification with the Data Steward is required to ensure the quality, integrity and security of data will not be compromised.

5.10 Data 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 in hard copy format must also be stored in a manner that will restrict access only to authorised user(s).

5.11 Appropriate data security measures (see Data Classification Policy and Procedure) must be adhered to at all times to assure the safety, quality and integrity of University data.

5.12 The definition and terms used to describe different types of data should be defined consistently across the University.

5.13 Data shall be retained and disposed of in an appropriate manner in accordance with the University's *Records and Archives Policy* and the *Records Retention and Disposal Schedule*.

6 POLICY REVIEW

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.

7 FURTHER ASSISTANCE

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

8 APPENDIX 1 DATA MANAGEMENT LIFE CYCLE