Data and Information Governance Procedure

Section 1 - Governing Policy

(1) This Procedure is governed by the Data and Information Governance Policy and supports ACU's broader policy environment. The Data and Information Governance Policy should be read in conjunction with this Procedure.

Section 2 - Purpose

(2) Information and data are valuable strategic assets for ACU. Efficient and effective use of information and data can drive quality assurance, continual improvement, risk management and the achievement of the ACU Mission, Identity and Values and ACU Strategic Plan. This Procedure has been developed to articulate the University's approach to data and information governance, in accord with associated policies and procedures.

(3) The purpose of this Procedure is to effectively and consistently manage information and data, while realising its value and mitigating adverse impacts on the University.

(4) This Procedure applies to all Institutional Data at ACU and each stage of the data and information management lifecycle, as referred to in the Data and Information Governance Policy.

Section 3 - Scope

(5) This Procedure applies to all ACU staff, contractors, third parties and consultants in their handling of institutional data and information in any physical, material or digital format.

(6) All ACU staff involved in the management, use and application of data shall ensure compliance with this Procedure and the Data and Information Governance Policy.

(7) Data management and governance shall be implemented in line with this Procedure and aligned to the Data Management Body of Knowledge (DMBoK) as far as is practical.

Section 4 - Roles and Responsibilities

(8) ACU, rather than any individual or Organisational Unit, is the owner of all data and information within ACU.

Role	Definition / Membership	Responsibilities
Governing Authority	Chief Operating Officer	Responsible for overseeing the approval, implementation and communication of the Data and Information Governance Policy and this Procedure across ACU.

Role	Definition / Membership	Responsibilities
Data Trustee	Member of the Senior Executive* *as listed in the Delegations of Authority Policy and Register - Management Levels 1 and 2	Data Trustees and their nominated delegates are responsible for: 1. overseeing the continuous improvement of the University's data and information governance and management; 2. verification of data and approval of data release and distribution to external parties as per the data verification process outlined in the Data and Information Sharing Statement (Part 4); and 3. management of data assigned within their respective portfolios.
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. **as listed in the Delegations of Authority Policy and Register - Management Level 3	Responsible for: 1. classifying data as per the Data and Information Classification Framework; 2. approving user access to their related data sources / sets (as per Section 6); and 3. assuring the requirements of the Data and Information Governance Policy and this Procedure are followed within their area of responsibility. under the guidance and direction of their respective Data Trustees.
Data Manager	Any member of staff with operational responsibilities in assisting Data Stewards or Trustees with day-to-day data administration activities. These include, but are not limited to developing, maintaining, distributing and securing institutional data. Data Managers are expected to have high-level knowledge and expertise in the subject matter and content of data within their area of responsibility.	Data Managers, as accountable to their respective Data Stewards, are responsible for: 1. fulfilling the responsibilities of their respective Data Stewards when such responsibilities are delegated to them; 2. ensuring effective local protocols are in place to guide and manage the appropriate development, distribution and use of data; 3. ensuring that a data trail is effectively documented (by email, system reports or project documentation) for their respective data sources / sets; and 4. providing guidance including adequate labelling of reports and data sets, explanatory notes, training and advice / assistance as outlined in Section 10 of this Procedure.
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.	Responsible for: 1. the quality assurance of the data that they gather, compile and distribute in primary reports and data sets; and 2. ensuring that a data trail is effectively documented (by email, system reports or project documentation) for their respective data sources / sets.
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.	Responsible for: 1. the quality assurance of how they apply data to develop subsequent reports, new data sets and other outputs; 2. when sharing / onforwarding data and reports, providing related explanatory notes and guidance to the intended recipients and where appropriate, referring recipients to the relevant Data Manager for further advice / assistance; and 3. ensuring that a data trail is effectively documented (by email, system reports or project documentation) for their respective data sources/sets

Section 5 - Classification Framework

(9) Please refer to the Data and Information Classification Framework for guidance on how data and information will be

classified in ACU.

Section 6 - Data and Information Discovery and Access

(10) Access to, and distribution / sharing of, information and data will be in line with the Data and Information Classification Framework and Data and Information Sharing Statement. Data will not be made accessible to any person unless the person has a genuine, work-related need for the data and meets the default access requirements for the classification of the required data as listed above. 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 if this information and data are solely of a general and non-sensitive nature.

(11) Subject to clause (17), approvals / permissions for any staff member to access any data or information from a data source will only be granted when the individual staff member requests access by lodging a Data Access Request ticket via Service Central and gaining endorsement by their respective member of the Executive for this request via the Service Now ticket. The endorsement requirement is waived when the staff member is at Executive Level or above (as listed in the Delegations of Authority Policy and Register - Management Level 3).

(12) Subject to clause (17), approvals / permissions for consultant and contractor access to data will only be granted when an individual staff member (as their contract manager) requests access by lodging a Data Access Request ticket via Service Central and gaining endorsement by their respective member of the Executive for this request via the Service Now ticket. In this instance, access will only be granted if the consultant / contractor has signed a non-disclosure agreement (NDA) (or equivalent) and this document is attached to the ticket.

(13) Upon endorsement by the relevant member of the Executive, the ticket will be forwarded to relevant Data Steward (or delegate) for:

a. assessing that the requestor meets the default access requirements for the data requested; and
b. approves or declines access as appropriate.

(14) The Data Steward (or delegate) may not unreasonably decline access if the requestor meets the default access requirements and has a genuine, work-related need to access the data.

(15) Data Stewards may delegate access decisions to a Data Manager in view of the associated risks and efficiencies and in view of the Data and Information Classification Framework.

(16) The ACU DataHub is a central source in ACU for data and reports. The ACU DataHub will enable direct access to data reports, information, guidance and training resources to facilitate and streamline data access. Requests for data access via the ACU DataHub will be facilitated by the ServiceNow processes mentioned above.

(17) Where appropriate, additional approval processes may be added to accessing specific data sources / sets where the basis of authority, reason and additional processes for such are documented and approved by the Responsible Officer and / or Privacy Officer (as appropriate). An example of such an additional approval process includes third-party access to personal information under the Privacy Protocol.

(18) Where appropriate, access to data may be facilitated using roles-based permissions embedded in source systems. Management of these role-based permissions will be approved by the relevant Data Stewards.

Section 7 - Data and Information Sharing

(19) Please refer to the Data and Information Sharing Statement on how data and information will be shared in ACU.

Section 8 - Data and Information Security and Protection

(20) Data and information stored in an electronic format will be protected by appropriate electronic safeguards and / or physical access controls that restrict access only to authorised user(s) in line with the Data and Information Classification Framework and the Information Security Policy and Information Security Procedure.

(21) Data and information in hard copy format will be stored in a manner that will restrict access only to authorised user(s) in line with the Data and Information Classification Framework and the Records and Archive Management Policy. Advice and assistance with records and archive management can be requested via lodging a Service Now ticket.

(22) Data 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 classification scheme.

(23) In the event there is a data breach relating to personal information, the Data Breach Procedure and Response Plan shall be followed.

(24) In the event there is an information security incident, the Information Security Policy shall be followed.

(25) In matters relating to staff and student personal information and data, the Data Privacy Policy and related procedures shall be followed.

Section 9 - Data and Information Quality and Integrity

(26) Data Stewards and their respective Data Managers are responsible for managing the quality of data that they develop and distribute, including:

a. the validation of their data prior to distribution; and
b. ongoing monitoring of data quality in their respective data sources including identification, logging and resolution of data quality issues.

(27) Assistance with fulfilling these responsibilities will be accessed from the Responsible Officer (or delegate).

(28) Data Users must take appropriate actions to uphold the quality and integrity of the data they access and the accuracy and validity of reports and outputs that they generate from applying the data. Such actions shall include gaining an adequate understanding of reports, data sets and explanatory notes and proactively accessing training and advice/assistance as outlined in Section 10 of this Procedure.

(29) Data in projects - appropriate and timely consideration must be given to data quality in projects, particularly as it applies to data migration and data integration. A formal component of every project requiring data must include early stage assignment of data roles, data profiling, analysis and planned rectification of poor data quality as part of data migration and data integration.

(30) Any system issues impacting on data quality shall be referred to the relevant Data Steward for the originating data source.

Section 10 - Data and Information Publication, Guidance and Training

(31) Data and information publication procedure – data providers (Data Stewards and Data Managers) are to provide adequate labelling, sourcing and explanatory notes in data reports / sets to enable effective and appropriate analysis, application and referencing. Assistance for providing this guidance / information will be accessed from the Responsible Officer (or delegate).

(32) Data Stewards will ensure that a data trail is effectively documented (define) for their respective data sources / sets in respect to the accessing, retrieving, reporting, managing and storing of data. Data Stewards may delegate this to their respective Data Managers as appropriate.

(33) Training will be provided by the Responsible Officer (or delegates) with the assistance of People and Capability for all ACU staff and included in the University's Learning and Development Plan through structured training (via webinars, workshops and online via the ACU DataHub).

Section 11 - Definitions and Terms

(34) 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.
Institutional Data and Information	All data or information developed and / or collected by the University in relation to its normal 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 Breach	Involves the loss of, unauthorised access to, or unauthorised disclosure, of personal information.
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 lifecycle.
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 and protection of University data in relation to the following criteria: access control; authentication; effective security incident detection, reporting and resolution; physical and virtual security.

Section 12 - Review

(35) This Procedure 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 this Procedure may forward their suggestions to the Responsible Officer.

(36) Unless otherwise indicated, this Procedure will still apply beyond the review date.

Section 13 - Further Assistance

(37) Any staff member who requires assistance in understanding this Procedure 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	Russell Parker Chief Information and Digital Officer
Responsible Manager	Pallavi Khanna National Manager, Data Excellence
Enquiries Contact	Pallavi Khanna National Manager, Data Excellence