Records and Archive Management Policy

Section 1 - Background

(1) This Policy establishes the framework for effective records and archive management at ACU. It provides guidance to ACU staff on the creation and use of records and sets standards for classifying, managing and storing those records. The Policy provides a basis for the management of information consistent with the ACU Strategic Plan.

(2) ACU has a substantial volume of Business Records relating to its teaching, research, students, staff, finances and other activities. The appropriate storage, retrieval and management of these information assets are required in order for ACU to efficiently conduct its business.

(3) A robust records and archive management program is fundamental to ACU's commitment to administrative transparency and accountability. It enables ACU to account for decisions and actions by providing essential documentary evidence and ensures the preservation of the institution's Corporate Memory.

(4) ACU is required to ensure that all aspects of its record keeping are managed appropriately. This Policy seeks to ensure that ACU's Business Activities are adequately documented through the creation of records that are managed in accordance with best practice and all applicable regulatory requirements.

Section 2 - Purpose

(5) The key purposes of this Policy and its related Guidelines and Protocols are to:

a. establish principles for the creation, management, storage and use of information at ACU;
b. define the roles and responsibilities for managing information appropriately;
c. ensure a consistent and effective approach to records and archive management; and
d. ensure adherence with applicable legislation and standards.

(6) Business Records are critical information assets required to support ACU's daily functions and operations. They provide evidence of ACU's core activities and establish Corporate Memory. Business Records support effective decision-making, collaboration, transparency and the achievement of priorities across ACU. To achieve this purpose, Business Records need to be:

a. accessible;
b. trustworthy;
c. appropriately governed; and
d. reusable.

(7) This Policy provides a framework designed to ensure Business Records are managed in accordance with these core principles.

(8) ACU is committed to compliance with relevant legislative instruments and best practice standards. It takes

responsibility for appropriately managing its Business Records throughout their entire information management life cycle. This includes, but is not limited to, ACU's obligations in relation to Information Management under Standard 7.3 of the Higher Education Standards Framework (Threshold Standards) 2021 (Cth) to ensure that information systems are maintained, securely and confidentiality as necessary to:

a. maintain accurate and up-to-date records of enrolments, progression, completions and award of qualifications;
b. prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity;
c. document and record responses to formal complaints, allegations of misconduct, breaches of academic or research integrity and critical incidents; and
d. demonstrate compliance with the Higher Education Standards Framework.[1]

[1] See Standard 7.3.3 (a)–(d) of the Threshold Standards.

Section 3 - Scope

(9) This Policy applies to all of ACU's functional units and campuses. It is intended to implement best practice by modelling relevant record keeping legislation in all States and Territories in which ACU has a presence.

(10) Business Records comprise both electronic (soft copy) and physical (hard copy) records and each type of record should be managed appropriately as part of a comprehensive record keeping program in accordance with this Policy and the associated Guidelines and Protocols.

(11) This Policy is part of a broader Information Governance Framework, which encompasses ICT governance, records and archive management and data governance and should be read in conjunction with policies and procedures in those areas.

Section 4 - Policy Statement and Key Principles

(12) Information is a key asset of ACU. Information assets are ordinarily captured in Business Records. These Business Records must be managed appropriately in accordance with business needs and external requirements.

(13) ACU adopts and enforces the following information management principles:

Information Management Principle	Definition
Create	Information created or received by ACU capable of being classified as a Business Record must be stored and managed in an Approved Business System. This management must be in accordance with internal policies, procedures, guidelines and external requirements.
Use	Information is an asset. Information classified as a Business Record must be accessible to staff consistent with their role and the function they need to perform.
Maintain	Information classified as a Business Record must be kept up to date and must be auditable and traceable. Appropriate security measures need to be applied to prevent unauthorised access, alteration, deletion or misuse.
Retain	Information classified as a Business Record must be retained for the relevant retention period or longer if there is a genuine business need, subject to overriding legislative restrictions (e.g.the Privacy Act 1988 (Cth)). These requirements are outlined in the Records Retention and Disposal Schedule.

Information Management Principle	Definition
Dispose	Information classified as a Business Record must be 'sentenced' (destroyed or archived) on a regular basis, as required or as appropriate. This activity must be in accordance with the Records Retention and Disposal Schedule (which considers regulatory requirements surrounding retention and disposal of records), protocol and business requirements.

Section 5 - Roles and Responsibilities

People

(14) Record keeping is an essential function of all staff. Every member of staff is responsible for creating and maintaining Business Records in order to fully and accurately record the functions, activities, transactions, operations, policies, decisions, procedures, affairs, administration and management of ACU in accordance with their roles.

(15) The Chief Operating Officer is responsible for ensuring that the University complies with its information management obligations.

(16) The Director, Legal, Assurance and Governance is responsible for oversight of ACU's records and archive management program.

(17) Records and Information Management Services (RIMS) within the Legal, Assurance and Governance Directorate is responsible for the oversight of ACU's records and archive management activities and will liaise with business system owners to ensure Business Records are managed in accordance with this Policy.

(18) The Chief Information and Digital Officer is responsible for ensuring that Approved Business Systems are appropriately installed, maintained and regularly backed up. Before a new system is considered for approval as per Schedule 1, the appropriate IT security assessment must be undertaken at the request of the proposed business system owner.

(19) Members of Senior Management, Management and Line Management[2] are responsible for ensuring appropriate systems and processes are in place for the capture, storage and disposal of Business Records within their areas of responsibility. They are also responsible for ensuring their staff are aware of their records and archive management responsibilities.

> [2] Management Levels 2, 3 and 4 of the Delegations of Authority Policy and Register.

(20) All staff and contractors of the University are responsible for creating and keeping complete and accurate Business Records in respect of their activities. Staff and contractors are required to follow authorised procedures when undertaking records and archive management activities. In addition, they must always observe security, privacy and confidentiality requirements in accordance with the Privacy Policy.

(21) Business system owners are responsible for capturing, storing and the subsequent migration or disposal of Business Records that are stored in any individual system that is not an Approved Business System. Such activities must be undertaken in accordance with the requirements of this Policy.

Systems and Processes

(22) Business Records must not be destroyed or disposed of without first undergoing a process of appraisal by the authorised officer responsible for the Business Record in consultation with, and upon the authority of, RIMS. Any

destruction process must be documented appropriately and must be performed in accordance with the Records Retention and Disposal Schedule.

(23) Strategies for digital preservation and migration must be in place for long-term digital information.

(24) Records and archive management requirements must be identified as a core requirement and assessed during system acquisition or development, and evidence of this assessment process must be retained in accordance with this Policy, the Procedures, and the Records Retention and Disposal Schedule.

(25) Records and archive management requirements must be included as a requirement and assessed when entering into cloud technology or similar service arrangements.[3]

> [3] Please refer to the IT Engagement – Procurement Process v1.5. This document may be revised periodically and is available upon request from the Office of General Counsel via Service Central.

(26) Any change in an Approved Business System must include a requirement for the transfer of Business Records consistent with the Records Retention and Disposal Schedule and authorised by RIMS.

Section 6 - Security and Access

(27) Authorised officers require access to Business Records to enable them to undertake the usual requirements of their role. Business Records must be made accessible to authorised ACU staff.

(28) The responsible officer for the relevant Approved Business System is required to ensure that all appropriate security and access controls are enabled and that staff using the Approved Business System are trained in the security and access requirements of the system.

Section 7 - Naming Conventions

(29) All Business Records need to be given clear and accurate titles. This is critical to make Business Records clear, easily identifiable and enables efficient search and retrieval processes that need to be undertaken.

(30) The key principles that should be applied when naming Business Records are described in the Naming and Titling Conventions Guideline.

Section 8 - Storage

Physical Records

(31) Business Records maintained as physical records should be stored in conditions that are clean and secure, with low risk of damage from theft, fire, water, dampness, mould, insects and rodents.

(32) Physical records should also be kept away from direct sunlight and other sources of light and heat.

(33) The storage area for physical records should be well secured, ventilated and ideally maintained at a stable temperature and humidity.

(34) Physical records should not be created, maintained or retained in circumstances where:

a. an electronic, digital or soft-copy version of the physical record exists; and

b. there is no legal, historical, archival or other need or requirement to maintain the physical record.

Records in Non-paper Formats

(35) Records in non-paper formats (optical media) such as photographs, computer disks or back-up tapes require specialised storage conditions and handling processes that consider their specific physical and chemical properties.

(36) Irrespective of format, records of continuing value require higher quality storage and handling to ensure long term preservation in accordance with the Records Retention and Disposal Schedule.

(37) Records in non-paper formats should not be created, maintained or retained in circumstances where:

a. an electronic, digital or soft-copy version of the record in non-paper format exists; and
b. there is no legal, historical, archival need or other requirement to maintain the record in non-paper format.

Section 9 - Disposal and Destruction of Records

(38) Staff may only destroy or dispose of records in accordance with the Records Retention and Disposal Schedule or in accordance with normal administrative practice as described in Appendix A of this document.

(39) The Records Retention and Disposal Schedule provides a listing of routine administration, legal, personnel, accounting, student and property records across ACU. It is mapped against relevant legislation in each state or territory in which ACU has a presence and should be accepted as the minimum retention period for records.

Destruction Protocols

(40) Business Records can only be destroyed using the protocols and authorisation outlined below.

(41) For destruction of physical records:

a. duplicate Business Records in physical (paper) format can be placed in security bins for secure destruction. They must never be placed in unsecured bins or rubbish tips. Destruction of physical Business Records needs to be authorised and organised by the RIMS team.

(42) Destruction of electronic Business Records should only occur with the authorisation of the RIMS team.

(43) For destruction of non-paper physical records (optical media):

a. destruction of non-paper physical records (including optical media) must be authorised and managed by the RIMS team;
b. where records are scheduled for destruction this should be undertaken by methods appropriate to the confidentiality status of the records;
c. all ACU Business Records approved and eligible for destruction must be destroyed under controlled conditions; and
d. if staff are uncertain of the status of a record, it should be treated as confidential and destroyed under confidential conditions. For further details, staff should consult the Records Disposal Protocol.

Section 10 - Application of this Policy

(44) This Policy applies to all Staff of ACU.

Section 11 - Review

(45) Directorates and campuses at ACU may be subject to audit and review to ensure compliance with the requirements of this Policy.

(46) To accommodate changes in legislation, technologies, programs and resources available to ACU, this Policy will be reviewed on a biennial basis.

Section 12 - Revision made to this Policy

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

Section 13 - Definitions

Term	Definition
Approved Business System	Any IT system or software that has been deemed a compliant system for management of information assets by the Director, Legal, Assurance and Governance in accordance with Schedule 1.
Business Activities	Any action that contributes towards ACU's decision-making processes or service delivery, including all of ACU's functions, processes, activities and transactions.
Business Record	Information Assets that are produced, received or retained by ACU in physical or electronic form in the initiation, conduct or completion of an institutional activity. It comprises content, context and structure sufficient to provide evidence of the business activity.
Corporate Memory	The accumulated body of data, information and knowledge created in the course of an organisation's existence.
Disposal	The destruction or deletion of Information from ACU's Approved Business Systems in accordance with the Records Retention and Disposal Schedule.
Evidence	Information (captured or represented in a Business Record or other record) that is used to prove a fact.
Information or Information Assets	Information (regardless of format) created, sent, received, and maintained as evidence and as an asset by ACU, in pursuit of legal obligations or in the transaction of business including (but not limited to) Business Records.
Information Governance Framework	The set of ACU policies, procedures and guidelines that define best practice in relation to information governance, including information security, data governance, records management, ICT governance, and privacy.
Information Security	The set of measures adopted by the University to manage risks to the confidentiality, integrity and availability of its information assets.
Retention	The retention and maintenance of information assets in accordance with the Records Retention and Disposal Schedule and Records Disposal Protocol.

Section 14 - Schedule 1

(48) The Approved Business Systems Guideline defines currently Approved Business Systems where ACU Business Records can be created, stored and managed in accordance with this Policy.

(49) Non-ACU Business Records (personal records) that need to be created and stored using ACU IT assets should be

saved in a staff member's personal OneDrive. Such use of ACU IT assets must be in accordance with the Computer and Internet Acceptable Use Policy.

(50) USB drives should not be used to store or transfer ACU information assets (in any format).

(51) ACU shared drives should only be used to store Business Records as an interim measure in the event of an emergency (e.g. if an Approved Business System is unavailable). These records must be transferred into the Approved Business System as soon as it is available.

(52) ACU Business Records should never be stored on computer desktops or computer C Drives. Desktop locations are not backed up, are not auditable and could lead to important information assets potentially being lost.

(53) For the purposes of this Policy, the Microsoft suite of collaboration products (including Outlook and Teams) do not constitute Approved Business Systems. This does not apply to any Microsoft software identified as an Approved Business System and listed from time to time in the Approved Business Systems Guideline. Business Records created in Microsoft Teams must be archived into the appropriately classified folders in the relevant Approved Business System immediately following the completion of the activity or project involving the Microsoft program.

(54) ACU One Drive for Business should only be used to temporarily store Business Records before they are moved or migrated into an Approved Business System.

Section 15 - Appendix A

Normal Administrative Practice (NAP)

(55) Destruction as a normal administrative practice usually occurs because the records are duplicated, unimportant or for short-term use only. This applies to both physical and electronic records.

(56) The following categories of records may be destroyed as normal administrative practice, subject to any contrary provision in the Records Retention and Disposal Schedule:

a. superseded manuals or instructions;
b. catalogues and trade journals;
c. copies of press cuttings, press statements or publicity material;
d. letters of appreciation or sympathy, or anonymous letters;
e. requests for copies of maps, plans, charts, advertising material or other stock information;
f. address lists and change of address notices;
g. calendars, office diaries and appointment books (other than those for senior management as covered in the Records Retention and Disposal Schedule);
h. facsimiles where a photocopy has been made;
i. personal telephone messages;
j. routine statistical and progress reports compiled and duplicated in other reports;
k. post-it notes with notes containing work content used to prepare other Business Records;
l. rough drafts of reports, or correspondence, routine or rough calculations not circulated to other staff in the organisation and of which a final draft has been produced and captured into an Approved Business System;
m. duplicates of other documents that have already been retained / archived.

(57) The key principles that should be adopted for NAP are defined in the Guideline for Records Disposal - Normal Administrative Practice.

Section 16 - Further Assistance

(58) All enquiries regarding this Policy should be directed to Records and Information Management Services, Legal, Assurance and Governance Directorate.

Status and Details

Status	Current
Effective Date	2nd April 2024
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	2nd April 2024
Expiry Date	Not Applicable
Responsible Executive	Diane Barker Director, Legal, Assurance and Governance
Responsible Manager	Diane Barker Director, Legal, Assurance and Governance
Enquiries Contact	Records and Information Management Services