# Records and Information Management Policy and Procedure

# Section 1 - Preamble

(1) Charles Darwin University (‘the University’, ‘CDU’) recognises and values its records and information as core strategic assets and is committed to achieving appropriate and ongoing management of these assets to advance the University's strategic priorities.

(2) The University will act responsibly to ensure that information is managed through its lifecycle and is available to the right person, in the right format and medium, at the right time.

(3) Good information management gives context and continuity for present and future staff and stakeholders, informs decision making, demonstrates accountability and transparency, and ensures the rights of the University community are protected.

# Section 2 - Purpose

(4) This policy and procedure:

a. outlines requirements for the governance and management of information at the University to ensure there is a consistent approach to creating and maintaining full and accurate records of all transactions and activities in accordance with good business practice and legislative requirements; and
b. specifies the core requirements for implementing fit-for-purpose information management practices to capture, manage, secure, store and deliver information to support key organisational processes.

# Section 3 - Scope

(5) This policy and procedure applies to all:

a. staff of the University and other members of the University community including contractors, consultants, authorised visitors, adjuncts, honoraries, volunteers, affiliates and third parties, and consumers who are connected to University networks, systems or services, irrespective of location or device ownership (eg on personally-owned computers);
b. information assets, in any format, created or received, to support University business activities; and
c. information contained in business applications used to create, manage and store information assets, including dedicated information management systems, business information systems, databases, email, voice and instant messaging, websites, and social media applications.

(6) Exceptions to this policy must be approved by the Chief Information and Digital Officer.

# Section 4 - Policy

(7) A record is defined as any information in any format created, received and maintained as evidence of any decision or action carried out by the University. These decisions and actions include all forms of the University's operational, teaching and learning, research, community service, organisational, commercial and cultural activities.

(8) The University is committed to creating, managing, retaining or appropriately disposing of all information that fully and accurately reflects its business activities. The University will comply with the Northern Territory Public Sector Organisations Records and Information Standards and align its practices to the Australian Standard for Records Management, AS ISO 15489-2002.

## Information Management Principles

(9) The University will:

a. follow standardised procedures for the appropriate capture, management, storage, archiving, or destruction of records;
b. ensure records are actively managed for their lifecycle to preserve context, integrity, and aid accessibility and usability;
c. follow procedures for the security, privacy and confidentiality of all records and information, and ensure that systems containing records and information are secure;
d. follow procedures for the storage of all records and information, in any format;
e. ensure records and information are made available in accordance with legislation and within the constraints of security, confidentiality, privacy and archival access conditions;
f. ensure records requiring retention and archiving in line with legal requests, pending or anticipated legal action or current disposal freezes are dealt with appropriately by Records and Archives;
g. ensure records disposal is documented with reference to approved University Retention and Disposal Schedules; and
h. never condone the falsification, alteration, damage, or removal of records.

## Roles and responsibilities

(10) All staff and members of the University community must comply with this policy and relevant procedures and create full and accurate records of University business activities they are responsible for, or are involved in, including records of all decisions and actions made in the course of official business.

(11) The Vice-Chancellor is the Information Trustee at the University. The Information Trustee is responsible for ensuring the ethical collection and management of the University's information.

(12) The Chief Information and Digital Officer has executive level responsibility for the management, implementation, and usability of information and computer technologies with the University to ensure these align with good governance.

(13) The Information Governance Architect is responsible for recommending information governance strategy and policy, leading the information governance program and promoting best practice in line with business need, legal requirements and professional standards.

(14) Records and Archives will:

a. create and keep up to date the Records and Information Management Policy and Procedure;
b. monitor policy compliance and make recommendations for improvement or modification of policy and practice;

c. administer and maintain the Corporate Records Management System, Content Manager, and conduct records management operations within the system;
d. ensure CDU staff and community are aware of their records management responsibilities, including by coordinating training and providing advice to staff as required;
e. provide advice to staff in relation to records and information stored in local business systems in order to reduce risk of non-compliance; and
f. review and maintain appropriate facilities for the storage of physical records and conduct auditing for quality assurance and data compliance.

### Systems requirements for managing records and information

(15) Content Manager is the University's approved Electronic Document Records Management System (EDRMS) and is used for records creation, capture and retention.

(16) Areas within the University that do not use Content Manager must ensure their day-to-day business activities and decisions are captured in a standardised way, in an authorised corporate business system with appropriate security, access and authentication controls and adequate retention storage capacity.

(17) Any business systems used to manage information should have the means to:

a. create and capture the content, structure, context and format of records. This includes requirements for the identification and aggregation of records;
b. maintain the authenticity and reliability of records. This includes requirements for access and security, retention and disposal, maintaining metadata and supporting migration and export; and
c. perform back up and restore activities and generate system reports.

(18) The following systems and/or tools do not provide adequate recordkeeping functionality and are not appropriate for use to manage or store University records:

a. Native email systems, such as Microsoft Outlook;
b. Local PC drives, portable storage devices;
c. Shared (network) drives; and
d. Third party services where there is no official University contract, such as Dropbox.

# Section 5 - Procedure

(19) A record can be any information in any format created, received and maintained as evidence of any decision or action carried out by the University;

(20) Managing Information through its lifecycle from creation to retention or disposal enables the University to meet its legal obligations under the Information Act 2002.

(21) Information lifecycle management includes the following phases:

a. Information creation, capture and management;
b. Information access and security; and
c. Information storage, retention and disposal.

## Information creation, capture and management

(22) Organisational information needs to be created or captured in a manner that ensures its integrity, quality and security. It is the responsibility of the staff member creating or capturing records to include any information unique to the record (i.e. metadata), that will assist in searching and locating the record. The following information should be included at a minimum:

a. proof of provenance - the owner or source of the record eg a person or Business Unit;
b. context that may justify an action, decision or outcome;
c. a title that describes the content using relevant keywords, a thesaurus, or titling conventions recommended by the relevant operational unit;
d. specific or unique identifiers, eg employee/student numbers, course or unit codes; and
e. dates or date ranges, version numbers.

(23) To avoid duplication, it is good practice for staff to refer to an organisational single source of truth to ensure that information being accessed is the most current. For this reason, saving a local copy of a file should be avoided.

(24) While email may be used in the short term, emails which discuss University business are corporate records and must be retained and managed in the University EDRMS or an authorised corporate business system for longer term storage.

(25) All hard copy records created or received by operational units should be stored securely to protect against theft, loss or damage, unauthorised access, alteration or falsification.

(26) An operational unit may convert hard-copy or non-digital records (i.e. audio, visual) into a digital format (i.e.image or scan) for the purposes of record keeping.

(27) Digital or electronic records and their metadata should be stored appropriately so that they remain accessible and usable for as long as they are required (including in legacy systems). Records that are created digitally (also known as born digital) are not required to be printed or have hard copies retained for the purposes of archiving.

(28) The University is obliged to meet a set of measurable requirements for the digitisation of hard copy records according to National Archives of Australia specifications. For information on recommended file format and compression, resolution and scanning requirements refer to Digitisation specifications for paper records.

(29) Digitisation processes must include quality assurance checks to ensure digital copies are fit for purpose for University business needs. The quality checks must include:

a. Checking each page to ensure it is readable and the context is clear;
b. All pages are present and accounted for; and
c. All pages are in the correct sequence.

(30) Risk prevention, response and recovery strategies for protecting and recovering vital University information in the event of a disaster are integrated into the University's Risk Management Framework and Enterprise Risk Management Policy.

(31) Any University employee is able to access appropriate records and Information management training and support to the level of their individual responsibility by contacting Records and Archives.

## Information access and security

(32) The University approach to information access is one of openness, encouraging a culture of information sharing to

ensure organisational effectiveness. Where required by legislative and/or operational requirements, information access will be managed appropriately in accordance with the University's information security environment to protect:

a. individual staff, student or client privacy; and
b. sensitive material.

(33) The Information Security and Access Policy outlines the University's commitment to implementing and maintaining a robust information security environment and provides further information on the safeguarding of information.

(34) The provision of access to information under relevant privacy and/or freedom of information legislation is contained in the Privacy and Confidentiality Policy.

(35) All members of the University should immediately report any suspected or perceived breach of privacy to the Privacy Officer.

(36) Staff leaving the University or moving roles within the University are responsible for ensuring records in their custody are made available to authorised staff. This includes transferring the custody of hard copy records, and ensuring electronic information stored in Outlook, personal drives such as One Drive and / or network drives have been archived in the University EDRMS.

### Information storage, retention and disposal

(37) The University is legally obliged to retain all records and information for the minimum retention periods according to legislative requirements and relevant governing legislation.

(38) the University will determine the actual retention period (which may be longer than the required duration) and these will be specified and published in the University retention and disposal schedules.

(39) Corporate information, regardless of format, must not be disposed of without proper authorisation by either destruction, deletion, transfer, sale or donation and without prior approval from Records and Archives.

(40) University records and information cannot be destroyed or deleted (disposed of) if:

a. they have not been identified in a University Retention and Disposal Schedule or relevant procedure and do not qualify under normal administrative practice;
b. the minimum retention period has not been met;
c. there is a current disposal freeze imposed on the records by the Federal or Territory Government; and/or
d. the University is aware of a matter, such as a legal case, which may require the records be retained.

(41) All records that are identified for disposal whether electronic or hardcopy must go through an approved disposal process managed by Records and Archives. This applies to any University records stored in legacy business systems.

(42) Information created such as notes, office messages, meeting requests, copies and duplicate records are considered short term and can be disposed of as part of normal administrative practice.

# Section 6 - Non-Compliance

(43) Non-compliance with Governance Documents is considered a breach of the Code of Conduct – Staff or the Code of Conduct – Students, as applicable, and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures outlined in the Charles Darwin University and Union Enterprise Agreement 2025 and the Code of Conduct – Students.

(44) Complaints may be raised in accordance with the Code of Conduct – Staff and Code of Conduct - Students.

(45) All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Policy and Whistleblower Reporting (Improper Conduct) Procedure.

## Status and Details

| | |
|---|---|
| **Status** | Historic |
| **Effective Date** | 20th April 2022 |
| **Review Date** | 20th April 2025 |
| **Approval Authority** | Vice-Chancellor |
| **Approval Date** | 20th April 2022 |
| **Expiry Date** | 27th April 2026 |
| **Responsible Executive** | Penny Szybiak<br>Vice-President Corporate |
| **Implementation Officer** | Cheryl Dias<br>Information Management Coordinator<br>+61 8 89467069 |
| **Enquiries Contact** | Cheryl Dias<br>Information Management Coordinator<br>+61 8 89467069 |

*This policy document may be varied, withdrawn or replaced at any time. Printed copies, or parts thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the Governance Document Library for the latest version.*