RECORDS MANAGEMENT POLICY AND PROCEDURE

CONTENTS

1 PURPOSE

1.1 This policy and procedure outlines how CQUniversity will manage records to meet business, legislative and regulatory requirements.

2 SCOPE

2.1 This policy and procedure applies to CQUniversity employees, and organisations and individuals acting as the University's agents, including any University controlled entities, contractors, consultants, and volunteers (referred to in this policy and procedure as 'employees').

3 POLICY STATEMENT

3.1 The University aims to establish and maintain effective and compliant records management systems to conduct business efficiently.

3.2 This policy and procedure will meet the following principles:

- recordkeeping responsibilities will be assigned and implemented to employees
- full and accurate records will be made, managed, and preserved for as long as they are required for business and legislative requirement
- approved information systems will ensure the systematic, comprehensive, reliable, timely and accurate retrieval of records (accessible records)
- records management systems and practices will be regularly monitored, audited, and evaluated for accountability, compliance, and continued improvement, and
- security provisions will be implemented to maintain record integrity and authenticity by preventing unauthorised access, damage, alteration, or misuse.

3.3 In the context of this policy and procedure, there are two types of records:

- records (also known as public records) – records that must be kept, and
- non-business related/ephemeral records – records that are of short-term value and are not required to be kept.

Retention and disposal schedules

3.4 The retention and disposal of records is governed by the *Public Records Act 2002* (Qld), and the following Queensland State Archives (QSA) Retention and Disposal Schedules:

- General Retention and Disposal Schedule
- University Sector Retention and Disposal Schedule
- Education and Training Sector Retention and Disposal Schedule.

3.5 The above retention and disposal schedules specify the minimum period that certain classes of records must be retained, and the conditions under which they may be disposed. Disposal of University records in contravention of these schedules is not permitted and is a breach of the University's compliance requirements.

3.6 The University may elect to retain certain classes of records for longer than the minimum retention period. Any such extensions will be specified in the relevant policy documents. Disposal of University records in contravention of these policy documents is not permitted.

Compliance

3.7 The Queensland Government Information Security Classification Framework (QGISCF) sets out detailed requirements for handling information according to its classification, including:

- preparation and handling
- removal from the workplace and monitoring
- discussing information
- electronic transmission

- copying and storage, and
- archive and disposal.

Sensitive information

3.8 Sensitive information should not be disclosed either due to its sensitive nature, because it has been received in confidence, or because disclosure might cause harm or be against the public interest, e.g. personal information, documents held 'In Confidence', and sensitive policy matters.

3.9 Sensitive information may be disclosed between individual employees on a 'need to know' basis, i.e. the information is required to undertake a business function or activity related to the University's core purposes. Any disclosure of information between employees must be in line with the reasonable expectations, or the express consent, of the person concerned. Any concerns about whether disclosure is appropriate should be referred to the head of the relevant business area.

3.10 Sensitive information (which includes anything classified 'xx-In-Confidence' or above) will be maintained under lock and key. Sensitive records will not be held in open-access conditions such as on a desk or computer desktop. Where practical, all files/records containing sensitive information should be retained in locked filing cabinets while not in use.

3.11 Sensitive information approved by the head of the relevant business area to move outside the University will be given the same level of security while off-site as it would have been had it been stored on-site. No sensitive information will be left unattended in a vehicle, public place, or in a non-secured container in a residence (including commercial accommodation). Records will be transferred in locked and covered receptacles to avoid accidental disclosure.

4 PROCEDURE

4.1 Records provide evidence of the University's business activities and/or conduct of affairs. Records kept on file will vary, according to the work undertaken. A record may be routinely created as a by-product of a business transaction, such as a receipt automatically generated by an online transaction, or deliberately created, such as a note or a phone call.

4.2 Risk-based decisions are used to determine what records must be kept or created to support business processes and activities. The following criteria may be applied when determining whether to keep or create a record:

- is the information needed to carry out business
- is there is a legal requirement to keep the information
- is the information required for financial purposes
- will the information be required to explain why a particular decision was taken
- will the information be required if a decision is challenged in legal proceedings
- will the information be needed to be publicly accountable and transparent for policy documents and decisions
- will the information assist to manage similar situations in the future
- is the information required to defend the rights and responsibilities of the University, its employees, or others, and
- does the information has value for historical, community or research purposes.

4.3 Duplicates or exact copies should only be retained if they contain significant annotations. They may be retained for local reference but should not be used to replace a formally created record. Duplicates should be clearly marked as 'copy' to distinguish them from the original records, and where possible, should cross reference to the original.

4.4 Drafts and working documents should be managed as a record where they:

- have been circulated for consultation with significant or substantial changes relative to a previous version

- include evidence of decisions or actions not contained in the final document, or
- include important annotations.

Emails and chats

4.5 Emails and chats identified as records must be captured into an approved information system. Microsoft Outlook and Microsoft Teams are not suitable systems to retain records.

4.6 Emails and chats (including attachments) identified as records must:

- be captured into an approved recordkeeping or information system. This includes business conducted via private email accounts
- include all parts of an email, such as attachments, links, graphics, and sound must be captured to retain the context, content, and structure of the email
- include email sequences (one or more replies) and email threads (forwarded to additional recipients) must capture the complete history of the communication to ensure that value of the record is preserved
- mitigate the risk of non-capture by waiting until the end of a sequence, capture should occur at significant points where decisions are made, the subject changes, or issues are addressed, and
- be captured by the creator of internal or outgoing emails, and the recipient of incoming emails.

Vital and high-risk records

4.7 Vital and high-risk records must be stored within the University's electronic document and records management system, Content Manager, as the single source of truth, and classified using the Business Classification Scheme. Shared network drives are not sufficient for storing vital and high-risk records.

Active records

4.8 Active records will be stored and managed within the relevant business area. Active records may be sorted and stored in whatever manner best facilitates their use.

Inactive records

4.9 Inactive records will be reviewed to determine if the minimum retention period has been met, in accordance with an approved QSA Retention and Dispose Schedule.

4.10 Where the minimum retention period has been met, records may be disposed of with appropriate approval as outlined in the disposal of records section of this policy and procedure.

4.11 Where the minimum retention period has not been met, records may be eligible for transfer to an archiving facility if the records have 12 months or more remaining on their retention period. Inactive records with less than 12 months remaining on their retention period must be stored and managed within the relevant business area.

4.12 Inactive records that have been assigned a status of 'permanent' under an approved QSA Retention and Disposal Schedule must be transferred to an archiving facility.

4.13 Where records are able to transferred to an archive facility, records must be prepared in accordance with the Archiving records section of this policy and procedure.

Creating records

4.14 Records may be created as a natural consequence of business, or as a deliberative action after an event.

- Full and accurate records must be created routinely to provide evidence of decisions and activities.
- Records that are not created as a part of a business process must be created as soon as practicable following the event.

- Security classification and labelling must be applied in accordance with the University's Information Assets Security Classification Policy.
- Physical records must be created on appropriate quality materials having regard to the likely use, and the required retention period of the records.
- Digital records must be created using a format that is likely to remain accessible and usable for the required retention period of the records.
- Business areas will ensure records are:
  - titled using standard terminology
  - classified and assigned a retention period using a QSA approved Retention and Disposal Schedule, unless no retention period applies under the Schedule at that time.

Capturing records

4.15 When a document is signed, or a decision is approved, the decision maker must return the document to the author or action officer to 'capture' the original document.

4.16 Capturing a record includes ensuring:

- information identified as a record is registered into an approved information system
- non-business related/ephemeral documents, as identified in the General Retention and Disposal Schedule, are not registered into an approved information system
- records are captured as soon as practicable after creation or receipt of the record
- records are attached to/within an identifiable file/folder
- records include minimum mandatory recordkeeping metadata in accordance with the Queensland Government Recordkeeping Metadata Standard and Guidelines. This includes (but is not limited to):
  - agent metadata: creator, recipient
  - record metadata: title, format, security, location, date created/registered, and
  - function metadata: business classification
- security and access controls are applied as soon practicable to limit access to employees with a legitimate 'need to know' basis
- records deemed vital to operations, or re-establishing operations in the event of a disaster, have business continuity contingency to ensure the record remains accessible and for purpose in the event of an emergency, and
- records that are born digital will remain digital where practical.

Using records

4.17 Employees must only access and use records which are necessary for the proper fulfillment of their duties or they have been instructed to access and use by law.

4.18 The preparation, transmission, handling, copying, storage, disposal, and discussions of security classified records must be in accordance with the standards set by QGISCF.

4.19 Records must be:

- handled with due care and in accordance with policy documents and associated information and resources available on the Records Management StaffNet page
- made available only to persons with a legitimate 'need to know', to fulfil their duties or contractual responsibilities
- stored in a secure information system that protects records from unauthorised access, damage, or misuse in compliance with Queensland Government Information Security Policy (IS18:2018), and

- released only in accordance with the Privacy Policy and Procedure and the *Information Privacy Act 2009* (Qld).

Releasing records

4.20 Records should not be released unless they are requested under a legislative directive. Refer to the Privacy Policy and Procedure for further information on the process to release records.

Sentencing records

4.21 The sentencing date will be used as a review date for considering whether the records have an actual or potential value beyond the minimum prescribed retention period. Sentencing a record does not set an automatic destruction date.

4.22 Examples of where records must be re-sentenced include:

- records involved in legal processes or accessed via the *Right to Information Act 2009* (Qld)
- the retention and disposal schedule under which the records have been sentenced has been superseded by a later version or new schedule
- action on a record has resulted in the record falling into a different disposal authorisation of the schedule, i.e. the subject matter changes from minor to major significance, or
- a record with a longer retention period than that assigned to the file is attached to the file, i.e. a minor complaint may develop into a formal inquiry.

4.23 When a file is re-sentenced, all existing parts must be reviewed as a complete record and re-sentenced accordingly.

5 STORING RECORDS

5.1 Records must be stored in an environment suitable to preserve them for the period required under the relevant retention and disposal schedule.

5.2 Factors to consider include:

- the records format (i.e. electronic, paper, film or photographs)
- how long the records need to be retained, and
- how often they will be accessed.

Electronic storage

5.3 Digital records should be stored in an approved information system that is:

- backed up regularly
- compliant with privacy and security requirements
- network or cloud based and allows for shared access
- organised in such a way that records can be identified and destroyed, with appropriate approval as outlined in the Disposal of records section of this policy and procedure
- able to migrate content to a new system upon replacement, and
- maintained through regular software updates (if applicable).

5.4 If a business area scans records with the intention of destroying the original paper document, please refer to the Digitisation section of this policy and procedure.

5.5 Digital records can only be destroyed (disposed/deleted) in accordance with the Disposal of records section of this policy and procedure.

Physical storage

Onsite

5.6 Business areas will ensure:

- location: sites, facilities and areas for records storage are located away from known hazards and are convenient to user needs
- structure: the structure of storage facilities protect records to ensure they remain accessible and useable for their required retention period
- environmental control: records are stored in environmental conditions that are appropriate to their format and retention period
- preservation: records are stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed for legislative and business requirements
- shelving and packaging: the shelving, equipment and containers for records storage ensure that records are secure, accessible, and protected from deterioration
- maintenance and security: records storage facilities, areas and records are maintained to safeguard their security, condition, and accessibility
- protection from disaster: emergency management and business continuity programs are established and maintained to ensure that risks to records are minimised and managed appropriately
- handling: the retrieval and use of records in storage areas are subject to controls that prevent damage and deterioration, and
- accessibility: records are stored and controlled in facilities where they can be identified, located, and retrieved easily.

5.7 Records storage facilities, shelving, containers, and equipment must comply with occupational health and safety requirements. Managers are responsible for ensuring compliance. Examples of compliant practice include:

- shelving positioned at reasonable heights, (i.e. waist to head height) and adequately secured to the floor or wall
- employees trained in manual handling practices and the correct use of shelving and equipment
- equipment available to promote safe handling of records
- boxed records do not exceed 12kgs to facilitate safe lifting practices, and
- record handling practices are monitored appropriately.

Offsite

5.8 The Records and Privacy Team will maintain a list of approved offsite storage facilities for records.

5.9 External storage facilities are subject to the same conditions in section 5.6.

Storage conditions

Preservation

5.10 Records must be preserved to ensure that they are accessible for as long as required. Preservation can be simple e.g. keeping paper files in a temperature-controlled room, or more complex, e.g. migrating electronic records to a new software platform to enable continued readability.

5.11 Preservation strategies will be influenced by:

- the need to constantly monitor and sustain appropriate environmental conditions over time
- how long the records need to be retained

- the facilities available for preserving temporary (short and long-term) and permanent records
- how quickly records need to be accessed, and
- relative importance of records for accountability, ongoing business needs, and cultural heritage requirements.

5.12 Digital records must be stored in an accessible and useable format.

5.13 Storage conditions must protect records from extremes of light, temperature and humidity, and must be well ventilated and insulated to maintain stable environmental conditions. Environmental conditions must be continuously monitored and sustained at appropriate levels over time.

5.14 Vital and high-risk paper records must be stored in a strongroom, vault or fire-rated safe. If these facilities are not available, other protection control methods must be implemented by the business areas, e.g. copies in separate locations, electronic back-up. Vital and high-risk digital records must be stored within Content Manager.

Location

5.15 Storage areas and facilities must be protected from potentially damaging magnetic fields that may cause loss or distortion of data in some record formats.

5.16 Records storage sites and areas must:

- have good drainage
- be isolated from internal hazards such as electrical plants and exposed plumbing
- have sufficient capacity for present and estimated future storage requirements
- be dedicated to records only
- be recorded in an identifiable information system
- be allocated within each business area where appropriate (for active records)
- be selected with regard to likely frequency and urgency of retrievals (for offsite record storage sites), and
- be located away from known risks such as hazardous industries sites e.g. explosives or chemical factories, gas and oil plants, flood or bush fire prone areas and locations which may be a target for vandalism.

Structure

5.17 Storage facilities, its services (e.g. electrical, plumbing) and/or storage areas must:

- comply with Australian building standards and codes
- be entirely weatherproof and sealed against dust, moisture penetration and the entry of birds and other pests and vermin
- have controlled access
- have sufficient floor loading capacity to cope with shelves full of records
- have ceilings that are high enough to allow clearance between shelves and fire sprinkler heads to ensure the sprinklers are not accidentally activated
- have a roof pitched sufficiently to ensure rapid rainwater run-off, and the guttering and down pipes should be appropriate and well maintained to prevent water overflow or blockages
- ensure windows or skylights are avoided so records are not subject to heat and light, and
- ensure doors are fire-proof and wide enough for ease of access of equipment.

Maintenance

5.18 The condition of records must be continuously monitored and remedial or conservation action undertaken. Contact the Records and Privacy Team if any of the following are present:

- infestation by insects or vermin
- dust, mold, or corrosion
- damage (such as rips or tears), or
- other forms of deterioration.

5.19 The Facilities Management Directorate is responsible for the maintenance of storage facilities. These areas must be constantly maintained, monitored, and inspected as part of an ongoing program (including regular pest control). Maintenance to facilities should be carried out promptly once problems are identified.

Protection from disaster

5.20 Storage conditions must protect both paper and digital records in accordance with this policy and procedure.

5.21 Disaster prevention, preparedness and recovery plans for records storage facilities and records must be implemented, tested, and understood by employees. Plans must be reviewed/revised when necessary or on an annual basis.

5.22 Risk must be identified and preventative measures incorporated in the design and management of records storage facilities.

5.23 Fire protection and suppression measures must be in place, including heat/smoke detection, fire alarms, extinguishers and sprinklers that comply with Australian Standards.

5.24 After recovery from a disaster, the cause must be identified, reported, and treated or managed, and the disaster prevention, preparedness and recovery plan reviewed and modified, as necessary.

Security

5.25 Storage facilities must protect records from unauthorised access, loss, destruction, theft, and disaster. Breaches of security must be reported to a manager, or in their absence the head of the relevant business area, and escalated to the Records and Privacy Team (email records@cqu.edu.au).

5.26 Local processes must be documented and implemented to ensure that access to record storage areas and records is restricted only to employees who require the information to undertake a business function or activity related to the University's core purposes.

6 ARCHIVING RECORDS

6.1 Inactive records, where the minimum retention period has not been met and there is 12 months or more remaining on their retention period, or have been assigned as 'permanent' under an approved QSA Retention and Disposal Schedule, may be eligible for transfer to an archiving facility. All records being sent to an archive facility must be managed through the Records and Privacy Team.

6.2 Records will not be retained for longer than required for business and legislative requirements to ensure the University is not exposed to unnecessary storage costs.

6.3 The privacy, confidentiality and security of archived records will be protected in accordance with the Privacy Policy and Procedure and *Information Privacy Act*.

Archive boxes

6.4 Archiving boxes from Grace must be used for records with a retention period of 10 years or more.

6.5 Grace archive boxes may be ordered directly from Grace, at the business area's cost.

Transferring records to archives

6.6 Physical records may be transferred to a University archive facility on the following conditions:

- prior approval has been received from the Records and Privacy Team
- records have more than 12 months remaining on their retention period
- where records transferred to a University archive facility have been misrepresented, and do not comply with the record requirements, the record owner will make those records compliant, and
- any and all costs associated with the collection and transportation of records to a University archive facility are the responsibility of the business area. There are usually no costs for re-locating records to a University archive facility on the same campus.

6.7 The Records and Privacy Team may transfer records to an inactive, intermediate, or offsite storage facility including an:

- onsite facility (a dedicated archive room)
- offsite facility on University premises (either owned or leased), or
- offsite facility on the premises of a commercial storage provider.

6.8 When determining where to transfer records, the Records and Privacy Team will consider:

- the demand for access to the records for ongoing business or urgency (vital records must always be available and easily accessible when required)
- the remaining period of time the records must be retained
- any special requirements i.e. record format or security considerations, and
- the cost of storage space.

Preparing records for archive

6.9 To a prepare a record for archive ensure:

- records are grouped together based on subject, activity and/or process
- extraneous materials are removed from the records, including rubber bands, paperclips, bulldog clips, plastic sleeves, lever arch folders, ring binders and display folders. Staples do not need to be removed
- records have been separated into one disposal class (document type) or a limited number of related disposal classes per box
- records are placed into archive boxes approved by the Records and Privacy Team. Refer to the Archive boxes section above for further information
- where batches of records need to be distinguished from one another within an archive box, use string, cardboard folder dividers, manila folders and/or cardboard document wallets only
- each box will contain only records with similar retention periods and disposal classes and must weigh no more than 12kg
- the approved Archive Box Label Form is:
  - provided to the Records and Privacy Team
  - placed inside each box, and
  - affixed to the short side of the box, draping over the handle holes.

Retrieval of records from archives

6.10 Access to the University's archives is restricted. Permission to enter archives must be sought from the Records and Privacy Team.

6.11 Requests to retrieve records from a University archive must be sent to the Records and Privacy Team (email records@cqu.edu.au). Upon receipt of a retrieval request, the Records and Privacy Team will conduct a search for, and arrange appropriate access to, the records. There are no costs for retrieving records and arranging access, except where offsite delivery of archive boxes is required.

6.12 Depending on the type of records, nature of the request, and resources available at the time access to records may be provided in the form of

- original documents, or
- electronic copies of documents.

6.13 Unless approval has been granted for permanent removal (disposal), records retrieved from a University archive must be returned once they are no longer required. Contact the Records and Privacy Team (email records@cqu.edu.au) to arrange the return of the records.

7 DISPOSING RECORDS

Disposal of records

7.1 Where the minimum retention period has been met, records may be disposed of. Disposal of records must be arranged through the Records and Privacy Team (email records@cqu.edu.au) and approved by the Director Governance (or nominee) as a delegate of the Vice-Chancellor and President.

7.2 Records must be reassessed prior to disposal to verify the accuracy of the original retention classification and determine any legal or business requirements necessitating a longer retention period.

7.3 Before determining if records can be disposed, the following must be considered:

- are the records correctly classified according to the subject matter
- is the assigned retention code current and accurately reflects the QSA approved schedule under which the records have been sentenced
- do the records have a social or cultural significance or any special security requirements
- are the records part of a past, current or pending court case
- do the records relate to risk management, public liability or insurance claims, and
- are the records of a contentious issue or a precedence-setting matter.

Disposal types

7.4 Employees will not bury records or place records in industrial bins, general collection rubbish bins or other unauthorised storage containers.

7.5 Physical documents must be placed in confidential destruction bins. Any physical documents that have been published or are available externally may be placed in a general collection rubbish bin.

7.6 For digital media requiring destruction, such as CDs, DVDs, thumb drives etc, please contact the Records and Privacy Team (email records@cqu.edu.au).

Disposal of non-business related/ephemeral records

7.7 Non-business related and ephemeral documents may be disposed of without requiring authorisation from the Records and Privacy Team. However, if there is any uncertainty as to whether particular documents or information constitute University records, employees should contact the Records and Privacy Team for advice prior to disposal.

7.8 Ephemeral documents in the public domain (i.e. promotional material, third-party publications) do not require secure disposal, and should be disposed into a standard waste or recycling bin.

7.9 Ephemeral documents containing personal and/or confidential information must be disposed of securely, as per sections 7.4-7.6 above.

8 DIGITISATION

8.1 Digitising records has many benefits, including greater accessibility, searchability and reduced storage and processing costs. However, it also has many risks such as accidental or deliberate deletion, erasure, corruption of the digital records, and poor-quality digitisation resulting in records that are not fit for use.

8.2 Eligible paper records may be disposed of after digitisation by identifying requirements to:

- assess original paper records for eligibility for disposal after digitisation
- apply appropriate technical standards during digitisation
- apply appropriate quality assurance checks on digitised records
- ensure the digital records are appropriately captured in an approved University information system, and
- ensure the destruction of original paper records is authorised and the paper records are appropriately destroyed.

8.3 This policy and procedure does not constitute a direction to destroy original paper records after digitisation, nor does it intend to mandate or otherwise limit digitisation occurring within the University.

8.4 The technical and quality assurance requirements may be applied as 'best practice' for any digitisation activities across the University, regardless of the eligibility of original records or information for destruction after being digitised.

8.5 Original paper records may only be destroyed if the following conditions are met:

Assess paper records for disposal after digitisation

- Records must have a temporary disposal status within a current QSA approved Retention and Disposal Schedule.
- Records that are covered by a disposal freeze, created before 1950, or have a permanent retention, may be digitised, however the original paper records cannot be destroyed.
- Records must be assessed as low risk for any ongoing legal or business requirements.

Digitisation

- Digitised records are captured and managed in an approved information system.

Quality assurance

- Equipment used for digitisation must be tested prior to use.
- Digitised records must be quality checked to ensure the digital record is a complete and 'fit for use' rendition of the original paper record.

Capture

- Capture must include additional digitisation metadata, including the date of digitisation, the equipment used for digitisation, and the person responsible for capturing the record.

Disposal

- Original paper records may only be disposed of by following the Disposing records section of this policy and procedure.
- A Request to Destroy Form must be accompanied with the Quality Assurance Checklist for digitised records when seeking approval to dispose original paper records.

9 RESPONSIBILITIES

Compliance, monitoring and review

Auditing records

9.1 Informal audits will be conducted by/under the direction of the Records and Privacy Team. Audits may include a desk-top audit (via survey) or a site visit.

9.2 Formal audits will be conducted by Internal Audit.

9.3 Informal and formal audit results will be discussed with the Director Governance and escalated to the relevant Committee for applicable action (if any). Audit feedback will be provided to the relevant business area/s for continuous improvement activity that is subject to ongoing review and assessment.

Responsibilities

9.4 The Vice-Chancellor and President, as Chief Executive Officer, is responsible for ensuring that the management of the University's records and information complies with legislative and regulatory requirements.

9.5 The Director Governance is responsible for implementing, monitoring, reviewing and ensuring compliance with this policy and procedure.

9.6 The Records and Privacy Team will:

- provide advice, tools and techniques for record-keeping best practices
- conduct informal audits to monitor recordkeeping for compliance with business and legislative requirements
- conduct searches and retrievals for information
- supply an effective and efficient records management system
- plan and control disposal programs for inactive records
- preserve and protect archival and vital records, and
- provide Content Manager training.

Reporting

9.7 The University must include details of its compliance with the *Public Records Act* in its Annual Report each year.

Records management

9.8 Employees must manage records in accordance with this policy and procedure. This includes retaining these records in a recognised University information system.

9.9 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

10 DEFINITIONS

10.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Active records: records that are still in frequent use, regardless of their date of creation, and required for current University business.

Approved information system: an approved system that has been assigned a Data Custodian and/or Application Custodian. Custodians are responsible for understanding, managing and controlling risks associated with application and the collections of data held within these applications. They are also responsible for ensuring that legal, regulatory, policy, standards and other business requirements of the application continue to be met.

Business classification scheme: a conceptual model of business activities, which identifies business functions and their associated activities and transactions.

Capturing records: registering the metadata about a record or transaction and saving the associated record and transaction into an approved information system. Refer to Responsibilities for capturing records for more information about who is responsible for capturing different types of records in different circumstances.

Content manager: the University's electronic document and records management system (EDRMS) used to manage documents and records throughout the document life-cycle from creation to destruction. Content Manager is an approved information system at the University.

Digital records: records created, communicated and/or maintained by some means of electronic or computer technology, including both 'born digital' records and records that have been digitised.

Digitisation: the creation of digital images from paper by scanning or digital photography. Digitisation disposal refers to digitising paper records so the original paper record can be destroyed, and the digitised record becomes the official record.

Disposal: in accordance with the *Public Records Act,* includes:

- destroying, or damaging the record, or part of it, or
- abandoning, transferring, donating, giving away or selling the record, or part of it.

Records disposal includes the following activities:

- destroy: complete and irreversible physical erasure of the records, ensuring it cannot be reconstituted, recreated, or reconstructed
- transfer: permanent transfer to another public authority because of a machinery-of-government change
- sell: records cannot be sold, except if an agency or function is sold or privatised (i.e. under a machinery-of-government change)
- donate: giving records to a museum or historical society must be authorised by the State Archivist
- loss or damage: because of a disaster or other circumstances beyond the agency's control, such as contamination
- abandon: neglect, which can lead to loss or damage to records, is a form of disposal, and
- amend: unauthorised changing of a record by addition, deletion, revision or obliteration of information, particularly if it modifies the meaning or intent of the record's content or renders it unusable.

Disposal freeze: the temporary cessation of the destruction of public records in relation to a specific topic or event, as issued by the State Archivist.

High-risk records: records that pose a significant risk to the University if they were misused, lost, damaged, or deleted prematurely. High-risk records may have one (or more) of the following:

- records that must be kept for greater than 30 years
- records of significant organisational change
- processes that are open to corruption or the potential of corrupt behaviour
- direct contact with individuals (i.e. a regulatory, enforcement, health, or welfare activity where there may be dispute), and
- a major program of international, national, or state significance.

Inactive records: records that are no longer required to be readily available for the University's current business.

Metadata: data that provides context or additional information about a record.

Non-business related/ephemeral documents: items of short-term temporary value that do not need to be registered into a University information system. A duplicate copy of a non-business related/ephemeral document may be treated as a record in some circumstances, as per section 4.3.

Physical records: a record that is tangible and takes up physical space (e.g. paper, photographs or index cards).

Record: in accordance with the *Public Records Act*, means recorded information created or received by an entity in the transaction of business or the conduct of affairs that provides evidence of the business or affairs and includes:

- anything on which there is writing
- anything on which there are marks, figures, symbols or perforations having a meaning for persons, including persons qualified to interpret them
- anything from which sounds, images or writings can be reproduced with or without the aid of anything else, or
- a map, plan, drawing or photograph.

Records may be digital or paper.

Record owner: An employee or business area who has overall responsibility for a particular record.

Sensitive information: a type of personal information which may result in discrimination or harm if it is mishandled. Examples of sensitive information include:

- race or ethnic origin
- religious beliefs
- membership of professional associations or trade unions
- sexual preference
- health information, and
- criminal records.

Sentencing: identifying the record class and applying the retention period.

Useable records: records that can be viewed and are fully functional and re-useable. If the user cannot view and/or use the information as it was originally captured then the record is not "useable", (e.g. its hyperlinks do not work). To remain useable, records must be maintained so that they can be quickly and easily identified and retrieved when they are required.

Vital records: records which protect the assets and interests of the University, generally associated with infrastructure, legal and financial matters, and without which, the University could not continue to operate. These records require significant resources (e.g. time and money) to reconstruct if they are lost or damaged or may be impossible to recreate altogether. Examples of vital records include:

- records relating to contracts, entitlements, leases, or other obligations required to recreate the University's legal and financial status
- meeting minutes with a legislative basis
- records relating to statutory and legislative responsibilities
- plans, designs, and drawings of major projects
- policy documents, licenses, and accreditations
- disaster management, including emergency preparedness and continuity plans

- records relating to core business operations
- delegations of authority
- records relating to current or potential litigation, and
- records that contribute to documenting the history of the University.

11 RELATED LEGISLATION AND DOCUMENTS

Information Assets Security Classification Policy

Information Privacy Act 2009 (Qld)

Privacy Policy and Procedure

Public Records Act 2002 (Qld)

Queensland Government policy documents (Queensland Government Enterprise Architecture):

- Records Governance Policy
- Information Security Classification Framework (QGISCF)
- Information Security Policy (IS18:2018)
- Recordkeeping Metadata Standard and Guideline

Queensland Government State Archives

Records Management StaffNet Page

- Archive Box Label Form
- Business Classification Scheme
- Information Sheet – Responsibilities for Capturing Records
- Quality Assurance Checklist
- Request to Destroy Form

Retention and Disposal Schedules (Queensland State Archives):

- Education and Training Sector Retention and Disposal Schedule
- General Retention and Disposal Schedule
- University Sector Retention and Disposal Schedule

Right to Information Act 2009 (Qld)

12 FEEDBACK

12.1 Feedback about this document can be emailed to policy@cqu.edu.au.

13 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Delegated Approval Authority	Chief Operating Officer
Advisory Committee	N/A
Required Consultation	N/A
Administrator	Director Governance
Next Review Date	09/09/2025

Approval and Amendment History	Details
Original Approval Authority and Date	Vice-Chancellor and President 10/03/2005
Amendment Authority and Date	Executive Director (Corporate Services) 26/09/2007; Vice-Chancellor and President 12/12/2011; Related documents updated 13/03/2012; Vice-Chancellor and President 26/06/2014; Vice-Chancellor and President 16/08/2017; Editorial amendment 02/09/2020; Vice-President (Student and Corporate Services) 09/09/2022; Editorial amendment 05/01/2023.
Notes	