Records Management Procedure

Policy Code: IM1697

Table of Contents

Purpose 1
Scope 2
Definitions 2
Capturing and Classifying University Records 2
What is a Public Record? 2
Staff Responsibilities 2
Managing Electronic Mail 3
Capturing Social Media 5
Access and Security of University Records 5
Access 6
Storage 6
Retention and Disposal of University Records 7
Managing University Records 7
Transfer Process - Partner Providers (onshore and offshore) 7
Cessation of Course / Program Delivery 8
Transfer Process - Ballarat, Gippsland, Berwick, Brisbane and Wimmera Campuses 8
Access to Records Stored Offsite 9
Disposal of University Records 9
Supporting Documents 12
Promulgation 12
Implementation 12

Purpose

As a public institution the University is bound by the Public Records Act 1973. Records received or created by University staff are deemed to be Public Records under the Act.

University staff including sessional staff, researchers and research staff are required to capture full and accurate records and manage and dispose of these records according to the authorised standards and records authorities issued by the Public Record Office Victoria (PROV).

Individuals who undertake work on behalf of the University, but are not employed by the University including -

- Partner Providers (onshore/offshore)
- Commercial Delivery
- VETiS (including Auspicing)

are required to ensure records they create and / or receive on behalf of the University are captured, managed, stored and disposed of in line with these procedures.

These procedures have been developed to provide guidance for the identification, capture, use, storage, security and disposal of records to ensure a consistent approach to records management across the University.

Scope

This procedure applies to all University staff and individuals who may perform work on behalf of the University, including:

- Partner Providers (onshore/offshore)
- Commercial Delivery
- VETDSS (including Auspicing)
- Sessional staff
- Volunteers
- Researchers, Research staff

and members of the University community who may create and / or access University records.

No staff are excluded from this procedure.

Definitions

For a full list of relevant definitions, please refer to the Records Management Policy

Capturing and Classifying University Records

What is a Public Record?

A public record is any information created by or received by an officer at the University that is evidence of a business transaction or activity. A Public Record records an action, policy, decision or decision making process, renders the organisation accountable or commits the organisation to an action. This information may be any hard copy, digital, email, sound or video recording that is evidence of a business transaction or activity. Examples include (but are not limited to):

- Student enrolment and administration documents
- Organisational management including strategic, operational and business plans
- Committees including minutes, agendas and papers
- Financial management including funding and financial transactions
- Research management including grants, project management and reporting
- Commercial activities including collaborations
- Governance including legal records
- Asset management including records of acquisition and / or disposal
- Contracts
- Human Resource management including staff files
- Patient records created and received by the University Health Centre
- Marketing and promotional material
- Program development including course approvals, materials and assessment content

Staff Responsibilities

Amendments to Records

To comply with mandatory PROV Standards and relevant legislation, it is the responsibility of all University staff to consistently create, capture, access, store and manage records as part of normal business practice. Corporate records must be handled, stored and disposed of in accordance with all relevant legislation.

The systematic capture of records in compliant systems ensures authentic, reliable and useable records are maintained as evidence of the University's business activities and transactions, allowing for better decision making, transparency and accountability.

All electronic records must be captured in an approved corporate business system. Records that are created by an approved corporate business system should be stored in that system. Records that are not created and / or stored in an approved business system must be stored in the corporate records management system, ECM. This includes but is not limited to email correspondence, word, excel and PowerPoint documents, video, audio, social media posts and telephone conversations (through recordings or file notes).

It is the responsibility of the Officer capturing the record to ensure sufficient metadata is included to enable other staff to easily understand when, how, where, why and by whose authority actions took place and decisions were made. [1] Business areas must ensure processes for the capture of records are documented and adhered to by staff.

Staff must not store records on network drives, laptops, temporary storage devices, portable drives, CDs, DVDs as these do not comply with recordkeeping requirements.

Staff must not use cloud technologies for the storage of corporate records. There are many risks associated with the use of the cloud for storing records including security, privacy, legislative compliance etc. Staff wanting to utilise cloud storage should contact Central Records and Mailroom services for advice.

Business system owners are responsible for ensuring their systems are compliant with Standards issued by PROV and the capture of records within these systems meet the requirements of PROV Standard 11/07 - Capture

Hard copy records must be placed on hard copy files and stored as per the *Records Management Procedure* - *Security and Access of University Records*.

Strategic Management Standard PROS 19/03– Issued by the Public Records Office of Victoria

In the event a document/record requires amendment to maintain accuracy, staff must identify the amendment to be made and document why the change was required, then sign and date the change. For physical documents put a line through and correct the data, for digital records keep a record of the amendment, including reason and who requested the change on file in Student HQ.

Managing Electronic Mail

Corporate Emails

Only business related emails should be captured in ECM. Business related emails are not to be archived using email client archive functionality or other archive management systems. Business related emails must not be stored on network drives.

Examples of business emails include:

- A direction relating to a course of action;
- An email that supports or gives meaning or context to a core business activity or transaction;
- The master copy of an agenda, minute, paper or report; or
- Business correspondence received from external sources

Emails created and sent using University systems must be professional at all times regardless of whether or not the email is considered to be business related or of an ephemeral nature. Emails which discuss University business are corporate records and may be required to be used in evidence (for example - appeals). Staff should ensure when creating email records they adhere to the requirements of the University's *Use of Computing and Communication Facilities Policy*.

Emails with Attachments

To ensure full and complete records are created, emails received by the University that contain attachments must be captured as a single record, that is the email message including the attachment must be registered into ECM. University employees must not register the attachment without the email message as this contains metadata which would be lost if discarded.

Email attachments sent from a University MFD (Multi Function Device).
Hard copy records which have been scanned using a University MFD and sent as an attachment to the registering officer for registration purposes can be registered separately and the email message discarded. This rule applies as the email message contains no relevant metadata to provide history or context to the attachment, and is purely a mechanism for delivery.

Short Term or Personal Emails

Emails of short term value used to facilitate University business, but are of an incidental nature or of such short-term value that they do not support or contribute to a business transaction, do not need to be captured and should be managed within personal email accounts. Examples include:

- Notices of meetings or copies of minutes;
- Copies of reports or newsletters; or
- External advertising material (or "junk mail").

Personal emails should not be captured in ECM. Personal email must be managed as per the *Use of Computing and Communication Facilities Policy*.

Note - Emails created and sent using University systems must be professional at all times regardless of whether or not the email is considered to be business related or of an ephemeral nature. Emails which discuss University business are corporate records and may be required to be used in evidence (for example - appeals). Staff should ensure when creating email records they adhere to the requirements of the University's Use of Computing and Communication Facilities Policy.

Responsibility for Email Capture

- Where an email is sent by a University Officer (either internally, or externally), it is the responsibility of the sender to ensure it is captured in ECM in a timely manner.
- Where the sender expects a reply, the sender can wait until the reply is received before registering the email. Where it is expected that it may be some time before a reply is received, the outgoing email should be captured and the reply captured upon receipt.
- Where an email is received from outside the University, the receiver is responsible for capturing the record into ECM.
- Where an email is received from outside the University and a number of University officers are included as recipients, the first officer named in the recipient list is responsible for capturing the record into ECM.

Capturing Social Media

Social media is the “term used for internet based tools for sharing and discussing information among people. It refers to user-generated information, opinion and other content shared and discussed over open digital networks” [1]

Social media may include (although is not limited to):

- Social networking sites (e.g. Facebook, LinkedIn, Myspace)
- Video and photo sharing websites (e.g. Flickr, Youtube)
- Blogs, including corporate blogs, personal blogs and micro-blogging (e.g. Twitter)
- Forums, discussion boards and groups (e.g. Google groups, Whirlpool)
- Wikis (e.g. Wikipedia)
- Video on demand (VOD) and podcasting
- Instant messaging.

Social media records created or received by staff in the course of their duties are public records. University staff must maintain accurate and reliable records of their official use of social media as required by relevant legislation, policies and procedures [2].

Social Media records can be captured by:

- Taking a screenshot of the post and adding it to a word document together with details of the context in which the record is used;
- Using a social media capture tool; or
- Using ECM Social Media capture functionality - refer to Central Records and Mailroom services for more information.

What should be captured?

- The content (the information that is sent or received) including representation of the format (text, visual, sound or video);
- The context in which the record is used, the business purpose of the social media record and its relationship to the business of the agency (purpose of the record);
- Where possible, the original content, otherwise a text log of entries;
- The metadata associated with the record, including the date and time the message was sent, the name of the Officer who authorised and / or sent the message, and to whom it was sent;
- For messages received by the agency, the name of the Officer and account that received the message, the purpose of the message (the relationship between the message and other records, why the message was sent or received, what it was in response to);
- The name of the social media application that the message was created on [2].

[1] State Services Authority 2010*, Guidance for use of social media in the Victorian Public Sector http://www.egov.vic.gov.au/victorian-government-resources/website-practice-victoria/web-2-0-victoria/guidance-for-use-of-social-media-in-the-victorian-public-sector.html*accessed July 2012

[2] Social Media Policy issued by the Public Record Office Victoria.

Access and Security of University Records

Access

Access to University records is only permitted by authorised University officers who require access for University business. Under no circumstances are records to be accessed or used for non-university related business.

Personal information held on corporate records must only be used for the purpose with which it was collected and must only be disclosed to authorised persons. Records containing personal information must be captured, stored, accessed, and disposed of in line with the requirements of relevant legislation (including, but not limited to the Information Privacy Act, Freedom of Information Act and Public Records Act).

Hard copy records stored within business areas must be secured to avoid possible theft, misuse or inappropriate access.

Business system owners must ensure systems comply with the requirements of PROV Standards. Business systems must be able to guarantee the security of records at all times and track who has accessed or amended data within those systems. Access to these systems should be reviewed on a regular basis to ensure compliance with PROV Standards 11/10 – Access.

University staff must ensure their username and password for University systems are kept secure at all times and are not shared with anyone else under any circumstances, as outlined in the University's Information Security Policy.

Responsibilities for staff leaving their position

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 records stored in Outlook and / or network drives have been registered in ECM.

Access to University Records by members of the Community including Staff

The Victorian Freedom of Information Act 1982 gives members of the community, including staff and students ("the applicant") the right to:

- Access documents about business of the university;
- Access documents about the applicant's own affairs and the activities of the University;
- Request that incorrect or misleading information held by the University, about the applicant's own affairs, be amended or removed [1]

Access to University records by members of the community or staff for non-work related, or personal reasons must be requested following the University's Freedom of Information (FOI) process. Refer to the Legal Office section of the Federation University website for more information.

[1] Freedom of Information - Federation University Australia - http://federation.edu.au/staff/governance/legal/legal-compliance/freedom-of-information

Storage

All hard copy records created or received by the business area are to be stored in PROV compliant storage areas within the business area while the record is being used for daily business activities. Active records must be stored securely to protect against theft, loss, misuse or inappropriate or unauthorised access [1].

It is the responsibility of the Manager of the business area to ensure hard copy files within their unit are stored securely and are only accessible by authorised University officers. Where records are required to be removed from their storage location appropriate procedures must be in place to ensure the tracking of those records.

Inactive hard copy records not required for normal business activities should be stored at the University's official offsite archive facility. Records are not permitted to be stored offsite at other non-University approved storage facilities. Transfer of inactive records must be completed as outlined in this procedure.

Electronic records must be stored in ECM, or another authorised corporate business system. Electronic records must not be stored in email clients such as Outlook, on network or local drives, portable storage devices such as USB sticks, external hard drives, CDs and DVDs, or other electronic recordkeeping systems.

Email messages must be recorded in ECM and must not be archived using email archive facilities. Storing electronic records in ECM will protect their integrity and authenticity as well as ensuring access by relevant University staff – refer to *Records Framework Procedure - Capturing and Classifying University Records* for more information.

[1] PROV Standard – Storage – Issued by the Public Records Office of Victoria

Retention and Disposal of University Records

Managing University Records

Hard copy records no longer required for normal business activities must be appraised by Central Records and Mailroom Services who will determine if they are to be transferred to offsite storage, PROV, or if they can be disposed of under a relevant RDA or NAP.

Hard copy records no longer required for daily business activity that have not met the requirements for disposal should be transferred to the University's offsite storage facility via Central Records and Mailroom Services. This facility has been assessed as being compliant with the Storage Standard (PROS 11/01) issued by PROV and ensures the preservation and security of the records until such time as they are ready for disposal or permanent transfer to PROV (for historically significant records).

Storage at other non-University owned offsite storage facilities is not permitted.

The following sections outline the process for requesting the transfer or disposal of records and is broken down into 4 sections:

1. Transfer Process - Partner Providers (onshore and offshore)
2. Transfer Process - Ballarat, Gippsland, Berwick, Brisbane and Wimmera Campuses
3. Disposal Process - Partner Providers (onshore and offshore)
4. Disposal Process - Ballarat, Gippsland, Berwick, Brisbane and Wimmera Campuses

Transfer Process - Partner Providers (onshore and offshore)

To request the transfer of Records:

1. Central Records and Mailroom Services should be notified via an email to centralrecords@federation.edu.au providing details of:

- the types of records to be archived;
- the approximate number of each type of record;
- the date range for each of record types;

2. Upon receipt of the request, Central Records and Mailroom Services will:

- provide advice regarding the retention requirements of the records and the relevant disposal authorities;
- provide advice regarding the preferred method for transferring the records to the Mt Helen Campus;
- email the *Archive Lodgement form*.

3. The partner is responsible for preparing and boxing their records.

Records must be boxed in C1 archive boxes. These boxes are available from most secure storage facilities - do not use archive boxes from Bunnings, Office Max, or other stationary suppliers as these boxes are not strong enough for storage requirements.

- where multiple record types exist, records are to be placed with similar records of the same class, or retention period.
- records containing sensitive or personal information are to be stored separately to records of a general nature.
- records are required to be removed from level arch files, bull-dog clips and plastic inserts prior to being boxed. Rubber bands or other methods of bundling are also not permitted to be used on records being prepared for archiving. Manilla folders or coloured paper can be used to separate records. Staples are permitted.
- The Archives Lodgement form is to be completed and a copy placed inside the top of each box.

4. Once boxed, records are to be transferred to Central Records and Mailroom Services at Mt Helen Campus. It is the responsibility of the sender to ensure records are transported in a secure manner.

Cessation of Course / Program Delivery

In the event that cessation of course / program delivery occurs prior to / or at expiry of contract, all University corporate records are to be transferred to the relevant school within 3 months via the Partner Providers (onshore and offshore) transfer process.

Transfer Process - Ballarat, Gippsland, Berwick, Brisbane and Wimmera Campuses

To request the transfer of Records:

1. The Business Area forwards an email to centralrecords@federation.edu.au providing details of:

- the types of records to be archived;
- the approximate number of each type of record;
- the date range for each of record types;
- the approximate number of archive boxes required.

2. Upon receipt of the request, RMS will (depending on complexity of the request / records) either:

- contact the Business Area to discuss the records and email the *Archives Lodgement form*.

3. The Business Area is responsible for preparing and boxing their records, ensuring:

- where multiple record types exist, records are placed with similar records of the same class, or retention period.
- records containing sensitive or personal information are stored separate to records of a general nature.
- records are removed from level arch files, bull-dog clips and plastic inserts prior to being boxed. Rubber bands or other methods of bundling are also not permitted to be used on records being prepared for archiving.
- the appropriate forms are completed and a copy placed inside the top of each box.

4. Once boxed, the Business Area emails Central Records and Mailroom services advising the boxes are ready for collection.

5. Central Records and Mailroom services will arrange for the collection of the boxes – paper work will be reviewed for accuracy and completeness prior to accepting ownership of the records.
6. Boxes are transferred to the Central Records and Mailroom services unit, where they are sentenced in accordance with the appropriate records management legislation and transferred to the University's offsite archive facility.
7. A copy of the *Archives Lodgement form* will be returned to the Business Area for their records.

Access to Records Stored Offsite

To request the return of a box from offsite storage, the Business Area is to email centralrecords@federation.edu.au with the details of the box/s to be retrieved.

Boxes can generally be retreived with 48 hours notice.

Disposal of University Records

University records must only be disposed of in accordance with an applicable Retention and Disposal Authority (RDA) issued by the Public Records Office of Victoria (PROV).

For the University, these are:

PROS 16/07 – Retention & Disposal Authority for Records of the Higher and Further Education Functions.

PROS 07/01 – General Retention & Disposal Authority for Records of Common Administrative Functions.

University records cannot be disposed of if:

- they are identified as having historical significance and / or are classed as a permanent record by PROV;
- they have not met the minimum retention timeframe as specified in the applicable RDA;
- it is known that the records may likely to be required in evidence, either now or in the future – regardless if a valid RDA has been issued by PROV;
- there has been an embargo placed on the disposal of records either by the University or PROV – regardless if a valid RDA has been issued by PROV;
- it is identified that there is still a business requirement for the records to be retained.

Electronic records undertake the same disposal authorisation process as hard copy records.

If you are unsure if the records you have are required to be maintained as corporate records, contact the the Central Records and Mailroom Services unit who will be able to advise you further.

Records Disposal Process

Prior to completing this process, an appraisal of the records should be performed, in conjunction with Central Records and Mailroom Services to ensure:

- the records have met their minimum retention period and are legally permitted to be disposed of;
- there are no legal requirements to keep the records either now or in the future – this may include current Freedom of Information (FOI) requests, legal proceedings etc.;
- there are no other legislative requirements to retain the records;
- the University has no further requirement for the records and;
- the records have no historical significance which would be lost by their destruction.

Records must not be destroyed where it is known that those records may likely be required in evidence, either now or in the future. This applies even where a valid Retention and Disposal Authority (RDA) has been issued by the Public Records Office of Victoria (PROV).

Penalties may apply to individuals identified as destroying records without appropriate authorisation.

Records Disposal Process - Partner Providers (onshore and offshore)

Records required to be retained for two or more years after business use has ceased should be forwarded to Central Records and Mailroom Services as per the Records Transfer Process.

Records with less than two years retention should be kept on site and disposed of using the process below. It is recommended that the disposal of records be conducted in conjunction with the yearly audits performed by University staff, who will review the records to be destroyed and complete the Central Records Disposal Checklist.

To request the disposal of records:

1. Central Records and Mailroom Services should be notified via an email to centralrecords@federation.edu.au providing details of:

- the types of records to be destroyed;
- the approximate number of each type of record;
- the date range of each type of record

2. Upon receipt of the request, Central Records and Mailroom Services will:

- provide advice regarding the retention requirements of the records and the relevant disposal authorities;
- email the Records Disposal Authorisation Form.

3. The partner is responsible for preparing and boxing their records.

Records must be boxed in C1 archive boxes. These boxes are available from most secure storage facilities - do not use archive boxes from Bunnings, Office Max, or other stationary suppliers as these boxes are not strong enough for storage requirements.

4. The Records Disposal Authorisation form is to be completed and signed by a Business Area Head and emailed back to Central Records and Mailroom Services.

5. The boxes should be securely stored until the yearly audit by University staff, who will review the records and complete the *Central Records Disposal Checklist*.

6. Once the checklist has been completed, it is to be emailed back to Central Records and Mailroom Services, who will review the checklist and arrange for *the Records Disposal Authorisation* to be signed off by the Manager, Registrar Services and the University Registrar (or their authorised delegate).

6. Once the *Records Disposal Authorisation* has been signed by all parties, the partner will be advised in writing via email that they can arrange for the secure disposal of the authorised records.

7. Secure disposal must be completed by the partner using a secure confidential document destruction bin provided by an authorised contracting company. Costs for the disposal of records remain the responsibility of the partner.

8. The site must obtain a destruction certificate from the contractor responsible for removing the secure bin to prove destruction has occurred. The destruction certificate is to be forwarded to Central Records and Mailroom Services to be stored with the original disposal authority form.

Records Disposal Process - Ballarat, Gippsland, Berwick, Brisbane and Wimmera Campuses

To request the disposal of records:

1. The Business Area forwards an email to centralrecords@federation.edu.au providing details of:
   - the types of records to be disposed of;
   - the approximate number of each type of record;
   - the date range for each of type of record;
2. Upon receipt of the request, Central Records and Mailroom Services will contact the department to discuss the records to ensure they satisfy the criteria for disposal.
3. Once Central Records and Mailroom Services have reviewed and ascertained the records can be disposed of, a copy of the *Records Disposal Authorisation form* will be emailed to the Business Area. This form will be required to be completed, signed by the Business Area head and emailed back to Central Records and Mailroom Services. .
4. Central Records and Mailroom Services will review the form and arrange for sign off by the Manager, Registrar Services and the University Registrar (or their authorised delegate).
5. Once the *Records Disposal Authorisation* has been signed by all parties, the Business Area will be advised in writing via email that they can arrange for the secure disposal of the authorised records.
6. Secure disposal must be completed by the Business Area using a secure confidential document destruction bin provided by an authorised contracting company, following the (BEIMS) Works and Maintenance Management System process. A request for a destruction certificate must be requested within BEIMS. . The details of a contact person is also required to ensure that the destruction certificate is delivered appropriately to the Business Area. Costs for the disposal of records remain the responsibility of the Business Area.
7. The destruction certificate is to be emailed to centralrecords@federation.edu.au to be stored with the original Disposal Authorisation form.

Destruction Methods for University Records

Destruction methods used must ensure the confidentiality of records at all times from point of collection to final destruction and destruction methods must be irreversible. Destruction methods should be environmentally friendly where possible. The burning, burying or disposal of records at a landfill site are not permitted. The destruction of records must be completed by an authorised contractor using authorised methods of destruction as specified in PROV Standard 10/13 - Disposal.

Acceptable methods of destruction include -

Paper records - Shredding and Pulping. Shredded paper must be pulped immediately after shredding to restrict the ability of shredded paper being reconstructed. Alternatively, paper records can be pulped without shredding [1].

Magnetic Media - records stored on magnetic media should be erased by degaussing (subjecting them to a strong magnetic field). Magnetic media can then be reformatted and reused. For sensitive records, magnetic media should be physically destroyed by shredding, corrosion or melting. Deletion of content is not a satisfactory destruction method [1].

Optical Media - Records stored on optical media such as CDs or DVDs should be destroyed by cutting or crushing [1].

Film and Microfilm - records should be destroyed by shredding, cutting, crushing or chemical recycling [1].

For the disposal of electronic records stored in Corporate Business Systems, Back-up systems or Hard Drives, contact Central Records and Mailroom Services.

NOTE - All records, regardless of format, must not be disposed of without proper authorisation as outlined in the **Records Disposal Process.**

[1] PROS 10/13 - Guideline 3: Destruction - issued by the Public Record Office Victoria (PROV)

Supporting Documents

Records Management Policy

Forms.

- Advice - ECM Naming Conventions (DOCX 219.7kb)
- Advice - Minimum Retention Requirements for University Records (DOCX 223.8kb)
- Federation University Archives Lodgement Form (DOCX 180.0kb)
- Federation University Certificate of Destruction (DOCX 216.8kb)
- Federation University Records Disposal Authorisation Form (DOCX 180.7kb)
- Federation University Records Disposal Checklist for Partner Providers (DOCX 217.9kb)
- Federation University Records Retention and Disposal Requirements (DOCX 755.0kb)
- Guideline - How to Lodge an Archives Box - Faculties and Departments (DOCX 292.7kb)

Promulgation

The Records Management Procedure will be communicated throughout the University via:

1. An Announcement Notice under ‘FedNews’ on the ‘FedUni’ website and through the University Policy - ‘Recently Approved Documents’ webpage to alert the University-wide community of the approved Procedure.
2. Inclusion on the University's online Policy Library.
3. Distribution of e-mails to Head of Schools / Head of Departments / School Business Managers, Business Area Managers, Executive Assistants and other stakeholder representatives;
4. Online Recordkeeping Awareness Training to be completed by all University staff.
5. Information sessions provided to staff by Central Records and Mailroom Services Unit.

Implementation

The Records Management Procedure will be implemented throughout the University via:
1. An Announcement Notice under 'FedNews' on the 'FedUni' website and through the University Policy - 'Recently Approved Documents' webpage to alert the University-wide community of the approved Procedure.
2. Inclusion on the University's online Policy Library.
3. Online Recordkeeping Awareness Training to be completed by all University staff; and
4. Information sessions provided to staff by the Central Records and Mailroom Services Unit.