

MANAGING UNIVERSITY RECORDS CREATED BY EMAIL

Policy Statement

University email accounts are intended for teaching, research and administration in support of the University's goals and objectives. Accordingly any email transmission residing on the University's computing and networking facilities is potentially an official university record.

The effective management of electronic mail transmissions is essential in order to permit the University to meet various legislative and accountability requirements, administrative needs, and to protect its rights and reputation.

The roles and responsibilities of the University's employees, defined by this policy, reflect the University's current paper-based record keeping system.

Introduction

A large proportion of the University's operational communication is carried out via electronic mail. Email is used for a wide range of purposes, including instructions, negotiations, authorisations, development of policies, employment matters, communications with students, advice of meeting arrangements, University announcements, and circulation of reports and committee minutes. Since most of these email communications are official records within the meaning of the *State Records Act 2000* and other applicable legislation, it is necessary to ensure they are effectively and efficiently managed.

The effective management of university records created by email supports administrative efficiencies by facilitating the identification and accessibility of records and by preventing the premature deletion of email messages relevant to management's decision-making. It also ensures that the University is able to meet requests for records required by the Auditor General, Ombudsman, Parliament, Royal Commissions, and under Freedom of Information legislation, thereby supporting organisational accountability.

Email transmissions may also be requested as evidence in legal proceedings or criminal investigations. Appropriate record keeping practices help to ensure the retention of relevant email messages and the ready identification and accessibility of these records. In the event of litigation involving the University, it would be necessary to assure the courts that email records presented as evidence, and the processes that created and maintained them, are reliable and trustworthy if they are to be permitted as admissible evidence. The application of this policy will help to provide those assurances.

This policy will assist staff in understanding their record keeping responsibilities relating to the management of email records and will permit the University to control the quality and quantity of its email messages. The completeness of the University's records will enable it to provide evidence of, and justification for, its activities and decision-making processes, thereby facilitating compliance with its legislative environment.

Definitions

Accountability

The principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others (including regulatory authorities, shareholders, and the public).

Central files	Central files are administrative files managed by the Records Management & Archives section and organised according to a subject-based Keyword Classification System.
Electronic mail	Electronic mail or email is defined as the transmission of messages over computer networks.
Record	Recorded information in any form, including data in computer systems, created or received and maintained by an organisation or person in the transaction of business and kept as evidence of such activity.
Records Management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including procedures for capturing and maintaining evidence of and information about business activities and transactions in the form of records.
Records Management System	An information system that captures, maintains and provides access to records over time.
Retention & Disposal Schedule	A records retention and disposal schedule is a systematic listing of the records series maintained by an organisation in which the period of time that each series is to be maintained or reviewed for destruction or kept for permanent archival retention is stated.
Retention Period	The period for which a record must be kept before it may be destroyed.
State Records Commission	The State Records Commission was established in 2001 under the terms of the <i>State Records Act 2000</i> . It is responsible for establishing principles and standards that govern record keeping by government organisations, and monitoring the operation of and compliance with the Act.

Purpose

The purpose of this policy is to establish a campus-wide policy on the management of electronic mail transmissions as official University records.

Scope

This policy applies to all staff that use the University's electronic mail system to create, receive, transmit, and retain information. This includes permanent, temporary and part-time employees, as well as contractors and visiting fellows.

1. LEGISLATIVE REQUIREMENTS

The *State Records Act 2000* ("Act") has specific provisions relating to the responsibility to create, manage and dispose of records in accordance with principles and standards issued by the State Records Commission. As an "incorporated or unincorporated body established or continued for a public purpose under a written law"¹, the University is subject to the requirements of the Act.

¹ Schedule 1, *State Records Act 2000*.

Electronic mail transmissions are included within the meaning of the Act's definition of a "record" which includes "*anything on which information has been stored or recorded, either mechanically, magnetically, or electronically*".

The principles and standards produced by the State Records Commission, in accordance with section 61 of the Act, represent the core record keeping requirements for agencies in Western Australia. These include the requirement to:

- Create and keep (in a suitable record keeping system) proper and adequate records of the University's business activity to ensure sufficient evidence of its performance of those functions
- Retain and dispose of records in accordance with approved retention and disposal schedules
- Support record keeping programs with policy and procedures.

Electronic mail transmissions are also subject to the following legislation:

- The *Freedom of Information Act 1992* provides a legal right for members of the public to have access to information held by public sector agencies, including universities. All university records, regardless of the media they are created in, are subject to disclosure under this Act
- The *Ombudsman Act 1976* grants power to the Ombudsman to request from the University documents or other records relevant to an investigation
- The *Electronic Transactions Act 2003* provides a regulatory framework that facilitates the use of electronic communications as a way of entering into transactions
- Under the *Evidence Act 1906* email communications can be subpoenaed for litigation purposes. The *Acts Amendment (Evidence) Act 2000* makes provision for the admission of evidence created using electronic media
- The *Criminal Code Act 1913* (section 85) has penalties for any public officer found guilty of damaging or destroying records or falsifying records by making false entries
- The *Financial Administration and Audit Act 1985* governs requirements for the management of financial and accounting records

All records that become subject to subpoena, court discovery, Freedom of Information or official inquiry by the Ombudsman or Human Rights & Equal Opportunity Commission (amongst others) must be identified and managed until action on the request, and on any subsequent internal and external reviews, is completed.

2. DETERMINING THE VALUE OF AN EMAIL MESSAGE

For the purposes of this policy email transmissions fall into one of the following 4 categories:

Personal email

Personal email messages have no relevance to the official business of the University and can be deleted at any time. Examples include lunch arrangements, jokes, and private messages between employees.

Spam emails

Unsolicited email messages that are not related to an employee's work responsibilities should be deleted immediately.

Information value only

Emails that relate to the business of the University, but intended only for informational value or to facilitate University business may be deleted once they are no longer needed. This includes:

- Email that is only relevant to specific Schools or Offices and where the email message has only temporary value. Examples include advice of meeting arrangements, advice of staff movements, copies of documents sent only for reference purposes, stationery requests, invitations, and staff leave requests
- Email messages received by courtesy copy and where no action is required. Examples include copies of committee minutes, reports, and newsletters
- Broadcast emails including Academic Council Announcements, General/Staff/Student Announcements, and Guild Announcements. The Records Management section will include broadcast emails in the record keeping system if they have ongoing administrative value.

Administrative email

As a general rule, emails received by or initiated by the University's employees and which relate to the business activities of the University and that have continuing administrative value to the University must be retained for as long as they are needed to meet administrative and legal retention requirements. Administrative email includes:

- Authorisations and instructions (e.g. to purchase office equipment)
- Commitments on behalf of the University
- Communications between the University's employees relating to official business
- Development or amendment of policies and procedures
- Emails that add value or support to an existing record
- Final versions of reports or recommendations prepared for management and external agencies
- Formal communications with external organisations
- Formal correspondence with enrolled students
- Formal drafts of agreements and legal documents and associated correspondence
- Minutes and agendas of committees and working parties
- Negotiations and commitments on behalf of the University
- Research matters
- Statistics and analyses
- Submissions to external bodies
- Where a precedent is created
- Where an email requires action from an employee
- Where legal advice is involved

3. ROLES AND RESPONSIBILITIES

The University's record-keeping system is primarily paper-based and, accordingly, email messages with continuing administrative value should be printed and filed. Email transmissions should be managed in a regular office filing system.

All University employees have a responsibility to create and keep records that adequately record the University's activities and should observe the following when constructing and managing their email:

- (a) Decide if individual email messages have value as official University records.
- (b) Prevent the premature deletion of official email records and delete them only in accordance with approved retention and disposal schedules.
- (c) Respect the confidentiality of email records and the privacy of personal information.
- (d) Protect email transmissions against unauthorised access.

- (e) Protect email records against alteration and manipulation.
- (f) Employees must decide if attachments should be kept, together with the email, as a record. In most circumstances the attachment should be included along with the email message to ensure that the meaning and completeness of the email is retained.
- (g) Retain the transmission data of email messages to ensure the integrity of the email as an official University record. This includes retaining the date and time of the message, sender and recipient details, subject of the message, and any attachments to the email.
- (h) Where email messages form part of an email conversation string it is not necessary to include each reply separately. Email strings should be included as records at significant points during the conversation or at the end of the email exchange.
- (i) Ensure the subject field is sufficiently descriptive about the content of the message to facilitate prompt identification of specific email messages.
- (j) Use folders based on function, subject or activity to manage email transmissions. Folders titled Annual Report, Budget issues, Conferences, Research issues, etc permit email to be more effectively managed than by using only the Inbox and Sent folders or organising emails by month or year. It also facilitates the efficient retrieval of messages relating to the same subject and allows for the systematic disposal of redundant emails to take place.
- (k) Include an appropriate signature (your name, position, and name of Office/organisation) and a disclaimer. The following disclaimer notice is provided as an example:

PLEASE NOTE:

This email and any attached files may contain confidential information and may be privileged. If you are not the intended recipient any use, disclosure, dissemination or copying of this email or the contents thereof is unauthorised. If you have received this email in error, please advise the sender by return email immediately and delete this message and any attachments.

- (l) Email communications with enrolled students, including scholarship and international students, should be printed and filed on the appropriate student file.
- (m) Email communications pertinent to an employee should be printed and filed on their personnel file maintained by the Office of Human Resources.
- (n) Where Central files are used to manage documentation employees should forward or send a cc of the email transmission to records@murdoch.edu.au or print and send the hard copy to the Records Management & Archives section for placement on the Central file.
- (o) Responsibility for deciding whether an email transmission is to be included in the record keeping system resides with the originator of the email. When email is received from outside the University it is the recipient's responsibility.
- (p) The Office of Information Technology Services has responsibility to copy to suitable media all email of staff that leave the employ of the University, including mailbox and personal mail files plus any files in the "Home" area, and to store these with their personal file in the Office of Human Resources.

4. RETENTION AND DISPOSAL

Standard 2, Principle 5 (Retention and Disposal) issued by the State Records Commission requires the University to retain its records for varying periods of time before they are disposed. Accordingly, email records with continuing value must be disposed in accordance with the retention periods indicated in the University's approved retention and disposal schedules.

The University's approved retention and disposal schedules incorporate all appropriate legislative, fiscal, administrative and archival requirements that must be considered when records are appraised for their retentive requirements. It should be noted that there isn't one single retention period that specifically covers all records created by email, as it is the information content of each email that must be assessed to determine its retention period. By observing these schedules employees:

- (a) Ensure they comply with legislative requirements
- (b) Ensure that records created by email are available for evidentiary purposes, to meet requests under FOI legislation and other discovery requests and judicial orders
- (c) Prevent the premature destruction of relevant records, thereby avoiding potential administrative or legal problems.

The retention and disposal of records created by electronic mail is a responsibility of all employees who send or receive email transmissions.

Records may be kept longer than the retention period indicated in the retention and disposal schedules but must not be destroyed before then.

When email records are subject to legal processes such as discovery and subpoena, they must not be destroyed even if the retention period has passed.

Personal emails and emails meant only for information value may be deleted at any time after they have been read.

Where a copy of an email record has been sent to the Records Management & Archives section, or printed and filed in a local record keeping system, the electronic copy may be deleted at any time.

The University's retention and disposal schedules are available at the following URL address: <http://www.murdoch.edu.au/vco/secretariat/records/retention.html>

5. ACCESS TO EMAIL RECORDS

- Electronic messages must remain accessible while they are required to meet administrative and external accountability requirements.
- Email records are official records that belong to the University and, subject to confidentiality considerations, should be available to any authorised staff member where the email has relevance to their work.
- Employees are required to protect personal or commercially sensitive information from unauthorised disclosure.
- University records created by email must be made accessible to authorised external agencies requesting them, and when required for legal proceedings. This is subject to any exemption that may apply, e.g. documents that are subject to client-lawyer privilege.
- All authorised staff are permitted access to records maintained by the Records Management & Archives section, except where records are classified as confidential and restricted. A staff member's right to access these records will be determined by their 'need-to-know' and their level of delegated authority, but authorisation from a member of the administrative executive may also be required before access is granted. The Records Management & Archives section maintains a log of borrowers of central files.

6. ENCRYPTION

The University's "Standards and Guidelines for all users of University Computing and Network Facilities" explicitly states: "*Sensitive confidential material should not be sent through the electronic mail system unless it is encrypted*".

Although email clients usually permit the sender of a message to indicate if the subject matter is unclassified, personal or confidential, email networks are, nevertheless, not completely secure and are vulnerable to breaches of security. Staff should therefore refrain from using email for communications of a highly confidential or sensitive nature, unless the transmission is encrypted.

Encrypted email transmissions should be decrypted or printed and placed in an envelope marked “confidential” before being forwarded to the Records Management & Archives section.

7. OUTCOMES OF EFFECTIVE EMAIL MANAGEMENT

- Adds to the corporate memory of the University, and results in better quality decision-making;
- Ensures official records created by email are available and accessible to employees;
- Evidence of decision-making and ability to defend decisions during litigation;
- Facilitates identification and accessibility of email transmissions requested by legal processes such as discovery orders and subpoena, or required by the Auditor General, Ombudsman, Parliament, Royal Commissions, and under Freedom of Information;
- Legislative and external accountability requirements are met, and penalties for non-compliance avoided;
- Prevents the illegal or arbitrary destruction of University records;
- Promotes sharing of information.

RESPONSIBILITIES:	
Responsible Officer	General Counsel & University Secretary
Implementation Officers	Records Manager/Archivist
Information Contact Officer	Records Manager/Archivist

RELATED MATERIALS/POLICIES:
Conditions of Use of Computing and Networking Facilities Email and Internet policy Email Censorship and Unwanted Mail