

---

## Records Management Policy

---

<b>Policy Approval Body:</b>	Academic Board
<b>Date Created:</b>	26th February 2010
<b>Policy Custodian:</b>	Dean of Engineering
<b>Policy Contact:</b>	IT Manager
<b>File Location:</b>	W:\Data - ALL.Standard\Policies and Procedures\EIT Policies and Procedures
<b>Location on EIT website:</b>	<a href="http://www.eit.edu.au/organisation-policies">http://www.eit.edu.au/organisation-policies</a>
<b>Review Period:</b>	Three Years
<b>Revision No:</b>	5.1
<b>Date of Revision:</b>	20 August 2015
<b>Date Approved:</b>	20 August 2015
<b>Date Commenced:</b>	20 August 2015

**Definitions :** **Record:** A record is information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in a transaction relating to education and business. (modified extract from AS ISO 15489 Records Management Part 1 sect 3.15). In the context of the EIT, this includes such records relating to employment, education, meetings, all correspondence internally and to external agencies (e.g. governmental educational agencies and course preparation), client and supplier records. This record may be located in multiple offices throughout the world relating to international transactions.

**Archives:** Records that are appraised as having continuing value and selected for permanent preservation are placed (building/room/storage area) where archival material is kept; an organization (or part of an organization) responsible for appraising, acquiring, preserving and making available archival material. With the increasing emphasis on electronic records (and the concomitant decrease in cost of electronic storage and increase in capacity), archives may also be electronic documents (or scanned facsimiles of paper documents), which are stored on site at the EIT campus and also stored off site (or “in the cloud”).

**Metadata:** Data describing context, content and structure of records and their management through time

**Records Management:** Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposing of records, including processes for capturing and maintaining evidence of and information about business activities and transactions.(Sourced from the AS ISO 15489 Records Management standard).



- Purpose:** The purpose of this policy is to establish a clearly defined process to create, manage and protect records including paper and electronic based records (e.g. email, DVD, hard disk and web sites). This policy allows EIT to meet its business, legal, personal and cultural obligations.
- Scope:** This policy extends to all EIT higher education staff, both administrative and academic, who handle records (as defined below).
- Overview:** EIT (and its sister company IDC Technologies) have a strong history of record keeping ranging from student records from over twenty years as well as over 130,000 client records built up as a result of business activities in over 200 countries in the world. This policy document covers recordkeeping and management systems requirements, responsibilities, creation, management and disposal of records. Other issues such as transfer of custody, security, access and details of student and staff files are covered. Finally, the policy of handling records when a disaster occurs is discussed in some detail.

**Essential Supporting Documents:** - AS ISO 15489 Records Management standard

- Related Documents:**
- Policy Development and Review Process Guideline
  - Policy Development and Approval Procedure
  - Procedure for Dissemination and Promotion of Policies and Procedures
  - EIT Marketing and Promotion of Courses Procedure
  - Risk Management Policy and Register
  - Award Nomenclature and Academic Records Policy
  - Recruitment, Selection, Appointment and Induction Policy
  - Selection, Appointment and Induction Procedure
  - IT Procedure Breakdown
  - IT Procedure Checklist

---

## 1. Introduction

EIT's Records Management Policy establishes records management systems which support the objectives of the EIT's Strategic Plan so that the EIT shows excellence in Management, Staff and Staffing processes.

Recordkeeping strategies and practices are developed and managed by the IT Manager, in consultation with the Policy Custodian, who provides ongoing support, development and training to enable EIT staff members to meet business needs, and legislative requirements.

In conducting its affairs, EIT implements many policy decisions which involve the explicit (and implicit) making and keeping of records. It develops and maintains recordkeeping systems that meet the requirements of the Australian Standard Records Management Parts 1 and 2 of the AS ISO 15489, 2002. It maintains records to meet its obligations under the applicable Commonwealth and State laws and the appropriate Australian standards.

Records are created to communicate information and in doing so provide evidence of how EIT acted on a matter. Records document policies and procedures facilitate actions



undertaken by staff to ensure consistency, establish corporate memory and provide an authoritative basis for establishing facts.

Not all documents created are records. Documents become records when they are evidence of a business transaction. For example, a Word document on a computer file becomes a record when it is sent (in whatever form – paper or electronic) to a colleague for advice or approval. As a record, it should be kept as evidence of that transaction for as long as the relevant retention and disposal schedule requires. This may be as short as a month, if it is arranging some minor task or for permanent retention if it forms part of a document presented to a meeting of the Academic Board or the Governance Board. However, with the rapid reduction in the cost of storage, coupled with the explosion in the volume of information and litigious nature of society, it is generally considered worthwhile backing up all documentation electronically for archiving.

## **2. Recordkeeping and Management Systems**

EIT's recordkeeping systems (which comprise staff, procedures and records management software) capture records, protect their integrity and authenticity, provide access through time, dispose of records no longer required by EIT in the conduct of its business, and ensure records of enduring value are retained.

EIT's corporate recordkeeping system is developed and managed by the IT Manager, in consultation with the Policy Custodian, who provides ongoing support, development and training to organizational units, so that the EIT's legislative, business and community responsibilities are met.

EIT's recordkeeping systems manage paper-based and technology-dependent records (including electronic (e-mail), micrographic and audio-visual) and websites. EIT's corporate system includes paper-based files of administrative, committee papers, staff and student records. Many of these are of enduring value because they capture EIT's decision-making processes.

## **3. Responsibilities**

The Dean of Engineering, as Policy Custodian, must ensure that EIT makes and keeps full and accurate records of its activities; and has regard for any relevant policy, standards and guidelines made by the WA State Archivist about the making and keeping of public records.

Senior staff, such as the E-Learning Manager and the IT Manager, are responsible for ensuring that adequate records are captured and maintained for use by authorised personnel in the conduct of their business.

The IT Manager is primarily responsible for the strategic management of EIT's record systems, for its records of enduring value, for developing policies and guidelines, setting standards, and for providing advice. In addition, the IT Manager is responsible for designing and implementing systems and communication and IT technology that complies with legislative requirements, meets business needs and ensures the integrity, confidentiality and availability of data.



The IT Manager manages records of enduring, permanent value which are no longer required for current administrative purposes. S/he provides storage, preservation and access to these records, observing relevant EIT policies, including Freedom of Information and Privacy principles. EIT is committed to abiding by the Australian Privacy Principles as described in Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, and to comply with the UK, South Africa, Canada, and US Privacy and Data Protection regulations where possible.

The E-Learning Manager is responsible for ensuring that staff create and keep records as an integral part of their work and in accordance with established policies, procedures and standards. They provide the resources necessary for the management of records and liaise with the IT Manager on all aspects of recordkeeping.

All staff within EIT who create, receive and keep records as part of their daily work, should do so in accordance with established policies, procedures and standards. Staff should not undertake disposal of records without authority and should do so only in accordance with authorised disposal schedules.

#### **4. Creation and Management of EIT Records**

Records play a vital role in the administration of EIT. Records provide reliable evidence of business transactions undertaken and contribute to administrative efficiency by ensuring appropriate evidence exists to support decisions and actions. Records form the corporate memory of EIT enabling facts regarding actual events, decisions and discussions to be retrieved when required. Once records are created, they need to be captured into an official record management system which ensures that the records are properly maintained over time.

All EIT staff members have a responsibility to ensure that:

- records are created to support the business activities with which they are associated
- records meet the needs and protect the interests of EIT, its students and other clients, and others affected by its decisions and actions
- records comply with legal obligations
- records support EIT in meeting its accountability requirements
- records of continuing value are captured and preserved.

Any record relating to the official business of EIT, created by a member of staff, is the property of EIT and needs to be dealt with in accordance with this policy.

Neglect or failure to ensure adequate records are made and kept may result in:

- disadvantage to clients (staff, students, stakeholders, members of the community)
- insufficient evidence to support decision-making
- inability to meet accountability requirements
- poor decision-making through lack of accurate records
- inefficiencies in administration
- time-consuming futile searches
- inadequate historical records of EIT



## **5. Disposal and Destruction of Records**

A person must not dispose of any record (including public records) unless the record is disposed of under authority given by the Dean of Engineering as Policy Custodian. The preferred method is simply to electronically back up all documentation if it is taking up too much critical (operational) space, especially on the EIT main server hard drives. In addition, paper-based records should be archived in EIT's secure storage locations.

EIT has an enormous amount of data which gets electronically backed up automatically on a daily and weekly basis. There is the possibility that the existing records can be overwritten unwittingly by a staff member and there is inadvertent loss of data which EIT staff may not become aware of until months after the loss of data. The principle to be followed with regard to all electronic records is thus that the IT Manager is responsible for arranging that all electronic data is placed on to a USB-based hard disk and transferred by the Dean as Policy Custodian to a secure location off-site for at least three months.

EIT has an obligation to ensure that no official records are destroyed without the prior permission of the WA State Archivist.

Destruction refers to the physical destroying of records contained in any media. A record may be destroyed only when it has no further value to EIT. This is determined systematically in accordance with an archives and records disposal schedule, which relates to written documents only and is maintained by the Accreditation Manager in consultation with the Course Coordinator.

Some records that no longer have relevance may nevertheless need to be retained, either permanently or pending their destruction. In such cases, they will be transferred to a secure location off-site for secondary storage.

The destruction of some public records is permitted without formal authorisation under normal administrative practice. This includes such items as drafts, spare copies and rough notes. If there is an uncertainty as to the nature of a document, the Dean of Engineering, as Policy Custodian, will be responsible for clarifying this issue.

Destruction of records should be done with due regard for privacy. Where possible confidential records will be transformed into an unreadable state, using appropriate technology.

## **6. Training**

The IT Manager is responsible for developing and maintaining appropriate training programs in records management for all staff within the EIT.

## **7. Transfer of custody of records**

At times, police investigations or EIT involvement in litigation will necessitate the transfer of official files or records out of EIT custody. This might occur in a case where the police service investigates allegations of criminal activity by a student when the allegations relate to EIT activities or functions.



Transfer of any official records or files (including academic and administrative records) out of EIT custody requires specific approval of the Chair of the Governance Board. A copy is retained for use, which ensures the integrity of the record and that the record remains available for the discharge of any relevant administrative accountabilities or functions.

All requests by external law enforcement agencies or by solicitors to obtain original EIT records should initially be referred to the Dean, as Policy Custodian, who will then refer the matter to the Chair of the Governance Board for final approval. In granting approval, the Governance Board should consider whether certified photocopies will suffice for the purpose for which the documents have been requested.

Where approval is granted, before any records leave EIT's custody, the IT Manager will be advised and appropriate arrangements made to ensure that EIT's recordkeeping responsibilities are fulfilled.

The IT Manager is responsible for monitoring the progress of the case to ensure that the original files are returned to EIT at the conclusion of the investigations or proceedings.

## **8. Security**

Documents and records created in the course of the business of EIT are the property of EIT. Staff should follow at all times EIT's Code of Conduct, and the policies and procedures relating to computing access which includes access to e-mail.

All records, whether paper or electronic, the latter including database information, media or web based records, need to be secure and not able to be altered. Adequate systems need to be in place to ensure that improper use cannot be made of documents or databases, or inappropriate access gained. It is the responsibility of all staff to ensure that EIT's records are of evidential value and that they properly reflect the transaction to which they refer and that they are unable to be altered.

## **9. Access**

It is expected that EIT's record keeping systems will provide timely and efficient access to and retrieval of records. It's systems will include and apply security controls on access to ensure the integrity of records is not compromised.

EIT staff are expected to access only those records and files which they need to fulfill the duties of the position to which they are appointed. All areas of EIT need to ensure that there are adequate systems in place to monitor access to EIT's records, and to ensure that records cannot be altered and that only staff with appropriate authority are given access. The IT Manager shall issue and update passwords and access details to defined individuals who require access to specific parts of the computer system. Anyone seeking access to areas other than their normal operating areas, shall request permission from the Dean of Engineering. Due to ongoing challenges in managing the IT security risk at an appropriate level, remote access to EIT's computer system shall not be provided to any external parties outside the physical location of the EIT premises and associated campus.



## **10. Donations of Non-EIT Records**

Records and Archives Management Services receives donations of EIT-related material which is of historical significance. These records become the property of EIT and are managed in accordance with terms and conditions negotiated at the time of deposit. This may include access or copyright restrictions.

## **11. E-mail and Electronic Communication Records**

E-mail (and instant messaging chat) records have the same status as paper records and should be preserved for similar periods. Where an authorised electronic document and records management system is in place (e.g. Microsoft Exchange), e-mails may be captured electronically into this system and managed as a record. Where no such system is available, paper copies of e-mails should be printed and a copy placed on the relevant file. All email messages should provide sufficient information so that the content is clear and that they can be properly classified to the relevant file.

## **12. Student files**

The files of EIT students contain information that relate to the student's admission, enrolment, progression and graduation in the various award programs of EIT. While a large amount of this information is captured and maintained in the student information system, the student file may provide additional information to support the processes.

Student records will be kept electronically for a minimum of 10 years. Paper records shall be kept for a minimum of 4 years, or 2 years after the student has graduated, whichever is greater..

Student assessments will be kept for at least one term after the previous term has ended. However, students' marks and grades shall be kept electronically for a minimum of 30 years.

For privacy reasons, some documents relating to a student or a prospective student should not be retained by any EIT departments. Instead they should be passed to the Financial Manager (also referred to as the Accounts Manager in older correspondence) to be stored in a secure manner. They include those aspects of a student record that contain the following information:

- Tax File number details
- Bank Account details and credit card details
- Passport details - should be sighted, noted as sighted in the student's record system and a copy made and saved on the system
- Birth certificates - should be sighted, noted as sighted in the student's record system, and saved on the EIT student's record system.

All records are subject to freedom of information requests.



### 13. Staff Files

An official EIT Staff File is established for all continuing and fixed term employees who commence employment with EIT. Each staff member's official file, together with the relevant payroll and financial system files, constitute the authentic record relating to the employment of a staff member, and evidence of that employment.

Staff files are paper-based files and many have lengthy retention periods in accordance with EIT's retention and disposal schedule. Current staff files are maintained by the Finance Manager rather than by the Human Resource Manager, as the number of staff members is small and unnecessary duplication of facilities is deemed inappropriate for the present size of EIT. All staff members are required to forward copies of any correspondence relating to staff employment activities of continuing staff to the Finance Manager. Copies kept for reference purposes should be destroyed when administrative use ceases.

The following documents constitute a staff file:

- Applications and associated documents relating to a successful application for an appointment at EIT
- Evidence of a staff members certificates, academic qualifications and awards
- Change of personal details, such as name and address
- Appointment correspondence (both offer and acceptance)
- Records of employment (e.g. start and stop of work)
- Requests for pay increases and altered employment arrangements
- Induction checklist
- Leave form records (including sick leave, maternity leave, etc)
- Worker's compensation and insurance claims
- Notice of termination of employment
- Correspondence, such as request for jury service
- Permanent Residence evidence
- Probation reviews, including deferment of probation due to inadequate performance
- Transfer from probation to permanent employment
- Training and education applications and results
- Redefinition and redeployment letters and associated correspondence
- Redundancy letter correspondence and notifications
- Resignation correspondence and acceptance (via a letter or email)
- Salary details, including loadings, additional bonus payments, per diems, travel, additional work request payments
- Superannuation details, including termination and transfers to another fund
- Additional workplace correspondence and agreements, such as EIT taking ownership of intellectual property and the appropriate compensation of a staff member.

All staff files are retained by the Finance Manager in a confidential location.

Due to the volume of applications, paper-based employment applications received that do not result in employment, will be destroyed within 30 days of receipt. However, electronic copies of these applications will be archived as they are on the email system which is extensively backed up.



Staff files, including those for casual staff, are retained and disposed of in accordance with the retention and disposal schedule authorised by WA State Archives. Normal practice is to keep such files for seven years in accordance with Commonwealth legislation (relating to tax and operation of a corporate entity). After this period, the file (if it is paper-based) will be destroyed.

#### **14. Board and Committee Papers – Agendas and Minutes**

This activity relates to the recording of the agendas, proceedings and minutes of the boards and the various official committees established and operating within the EIT and include:

- Governance Board
- Academic Board and its sub-committees (such as the Course Advisory Committee and Board of Studies)
- Ad hoc committees of EIT

The appropriate policy contact (such as the Accreditation Manager or the IT Manager) will manage the papers for committees appointed by the Governance Board or the Academic Board. Committees serve an advisory function and the records of their meetings should be held in accordance with EIT's retention and disposal schedule.

Board and Committee papers of EIT's organisational structure are of enduring value and must be transferred to the IT Manager for permanent retention. When issues arise that have an immediate or potential bearing on EIT policies and procedures, they should be noted in the policy issues log, maintained by the policy custodian, for the purpose of identifying issues that emerge through the implementation, the use and the review of policies.

As specified in the Policy Development and Review Procedure, outcomes of Board meetings or committee meetings that have a bearing on EIT policies and procedures also need to be recorded in the Communication and Implementation Plan relevant to that area of policy, which is overseen by the policy custodian in consultation with the appropriate policy contact. As well, the approval date of any revisions to policies or procedures should be recorded in the policy directory.

#### **15. Technology-Dependent Records**

Technology-dependent records, including electronic records, micrographic records and audio-visual records, generated or received in the course of business are public records and are created, maintained and accessible for as long as they are required to meet legislative, accountability, business and cultural obligations.

E-mail messages which are evidence of business activities are retained as records, with relevant contextual detail. These details include, as a minimum, the name of the author, the author's position title, the name and address of the organisation they represent, the name of the receiver, the receiver's position title, the name and address of the organisation they represent, the date and time the message was sent or received. Ephemeral messages of information-only value and private messages which do not provide evidence of a business transaction are not necessarily captured.

## **16. Audits**

Besides informal audits, regular audits shall be conducted by the IT Manager on at least six monthly intervals to ensure this policy is being followed. This includes initial and follow-up audits, as well as encouraging self-assessment of other managers to identify risks and areas of improvement. Where there is evidence of systemic non-compliance with the Records Management Policy, the policy custodian shall be advised and will take appropriate corrective action and report the problems as well as corrective action to the Governance board.

## **17. Risk and Disaster Management with Regard to Records**

### **17.1 Introduction**

Risk and Disaster Management as a general category is considered at a higher level within the organization structure of EIT, set out in the Risk Management Policy. The specific topic of this section of the Records Management Policy relates to the risks and disaster management of EIT's records.

Each area of EIT should ensure their records are protected from risks that may result in loss, damage, inaccessibility or unauthorised access or disclosure, which can:

- damage (or destroy) records of student's efforts
- damage (or destroy) staff records
- undermine the effectiveness of EIT's operations
- breach legal requirements
- create difficulties in supporting EIT or stakeholders' rights
- damage EIT's reputation.

The risk management in this area is particularly critical as a considerable amount of EIT education and educational processes are conducted remotely and in an online manner.

Some risk management processes are built into EIT's Record Management Policy. However, there are other risk factors that may affect records and recordkeeping systems locally which may not be evident through this process. e.g. a disaster such as fire or flood which destroys the entire EIT building and campus or a localised failure of the entire IT system due to a lightning strike. Each operational area of EIT is responsible for assessing risks that may affect the records they manage locally. This is particularly important for areas that manage centralised collections.

The information in this risk and disaster management section is designed to:

- identify existing strategies that minimise risks to records and recordkeeping systems
- assist individuals and business units to consider risk that may affect records within their area
- enable business units to take action against identified risks where possible
- enable business units to take action to reduce the affects of a disaster which may affect their hard copy records.



The risk and disaster management section includes:

1. Assessing record-related risks
2. Responding to a disaster
3. Recovering records
4. Post-recovery review

## **17.2 Risk Management Programs for Records**

The EIT Records Management Policy is in itself a risk management tool. The Records Management Program ensures sound recordkeeping practices that support business activities, assist in the capture and maintenance of corporate memory, and ensures compliance with relevant legislation

EIT's Records Management Policy is designed to prevent:

- inability to identify the existence of records
- lack of full and accurate records of business activities and EIT administration
- loss or inaccessibility of documents, including emails, letters, reports, etc.
- lack of documentation detailing verbal decision making processes
- lack of control over access to records
- inability to locate records or track their movements
- premature destruction of records without appropriate approval or retention of records without documented reason.

## **17.3 EIT Vital Records Program**

The Vital Records Program at EIT is a specific risk management tool. It is designed to prevent the loss of critical records (i.e. contracts, agreements and other records) by lodging them with the IT Manager for scanning (if required) and secure off-site storage.

The Vital Records Program is designed to prevent:

- loss of vital or critical records
- unauthorised access to vital records
- litigation or financial loss etc resulting from the inability to produce vital records when required
- inability to effectively operate in the event of a disaster.

## **17.4 Repository and archive management program**

EIT's archive repositories are managed by EIT Records. The repositories provide storage for short and long-term records of value that are required to be retained for a set period of time, as well as permanent EIT and State archives.

EIT Records repository and archive management procedures are designed to prevent:

- unauthorised access to storage areas and records
- damage or alteration of records
- loss of records
- indefinite retention of records
- premature destruction of records
- deterioration of records



- obsolescence of technology or inaccessibility associated with technology-dependent records.

Regarding archiving for electronic records, 5 weeks' worth of backups are kept, rotating the external backup hard drives weekly. The newest set of backups is always taken off-site every week in case of physical damage to the office premises. Every 3 months, one set of backup is taken permanently off-site for safekeeping.

### **17.5 Destroying records**

EIT has clear requirements for the destruction of official records. Staff are required to consider legal, administrative, financial, audit and specific legal retention timeframes before destruction of records can be authorised.

EIT's destruction procedures are designed to prevent:

1. premature destruction of records
2. insecure destruction of records
3. inadequate documentation of destruction activities.

### **17.6 Assessing records-related risks in specific EIT organisational areas**

Although some areas of risk are incorporated into the Records Management Program's audit and self-assessment activities, it is important for areas to be aware of other risks that may affect records or recordkeeping systems in their area.

It is particularly important for areas who manage centralised records to ensure a risk assessment is undertaken.

Risks affecting records and recordkeeping systems include, but are not limited to:

- building works (both minor and major)
- internal disasters (e.g. broken pipes, fire, electrical surges)
- external disasters (e.g. flood, earthquake, terrorism, lightning strikes)
- human error
- lack of policy and procedures
- use of inadequate storage areas (e.g. poor security or environmental conditions).

Staff should undertake an assessment of risks in conjunction with the Records Management Program audits and their self-assessment activities. As with the self-assessment process, the following risk assessment can be done at any time.

### **17.7 Preparing for a disaster**

To prepare for a disaster in advance and minimise the disruption it will cause, the following information will be saved on the server in a spreadsheet format (updated whenever staff changes occur) and kept in a safe location off-site by the Dean:

#### **Contact details**

A list of all staff responsible for assisting in records recovery will enable the area to contact staff quickly in the event of a disaster.

#### **Records Recovery Priority List**

An up-to-date Records Recovery Priority List will assist areas in identifying priority records during recovery operations. Such paper based records may include:



- those important to continue current and ongoing business
- vital records not yet lodged with EIT Records or on loan
- original student, staff or other client records held
- unprocessed student assessment and exam scripts.

The Records Recovery Priority List should be maintained by the policy custodian and should identify the records and where they are located. The list needs to be maintained regularly to ensure new records are added and location details are current. Most records on the list would already be classified as official records and as such, would be listed in the area's Records Database.

All electronic details should be backed up on a continuous basis using the latest server technology and these materials are removed from site at least once per week. This means that a working system can be set up on new computer hardware within 4 hours of a disaster occurring (assuming that power and an appropriate location to operate from is available).

This information should be retained within the office AND off-site so that staff can access it easily in the event of a disaster.

*Note: for the purposes of disaster recovery, 'off-site' is anywhere outside the building in which the area and its records are located. A different building, which can be accessed in the case of a disaster, is a preferable option.*

### **17.8 Responding to a disaster affecting records in specific EIT organisational areas**

This section considers responses to a disaster that affects physical records within an area. For all matters to do with IT systems and hard drives, the IT Manager will be the key contact.

#### **Responding to a disaster involving an evacuation**

The following actions should be taken in response to a disaster affecting hard copy records in your area in the event of an evacuation:

- Follow the EIT evacuation procedures. Protection of life is a priority over the recovery of records.
- If a disaster has or is likely to damage hard copy records, inform the Dean of Engineering or Human Resources Manager (whoever is around at the time of the disaster).
- If the affects of the disaster cannot be managed with in-house resources, the Emergency Management Team may bring in external disaster recovery specialists.

#### **Responding to a disaster not involving an evacuation**

There may be incidents in areas where life or health are not considered to be at risk and evacuation may not be called, however records may still be affected. For example, a leaking pipe over a storage unit or a leaking water cooler flooding the floor may affect records.

If records are affected the following action should be taken:

- Safety first - Assess safety of the affected area. Even though an emergency has not been called, safety may still be an issue.
- Prevent further damage - If the records are still at risk, move them from the affected area or eliminate the damaging factor.

- If the problem affecting the records is a building issue (such as a leaking pipe), contact the Office Manager immediately.
  - Move records to an area where they can be assessed and recovered.
  - If records are in boxes, move the whole box if safe and practicable. Use trolleys where required and be aware of manual handling issues.
- Dealing with document damage - If possible, staff should make a photographic record of the damage. Using a digital camera or mobile phone to obtain 'before' and 'after' photographs can provide a record of recovery operations for use in the post-recovery review. It may also be important if an insurance claim eventuates.
  - Plan recovery - Staff should locate their area's Records Recovery Priority List or other record lists. Each area should have a specific Records Recovery Priority List maintained by the IT Manager. These lists should be developed and maintained as part of the disaster preparedness plan. Key recordkeeping areas of EIT are obliged to maintain such a list.
  - Local recovery of records - Some recovery operations can be managed locally by staff within their own area. If the disaster is beyond the resources of the area to recover, staff should contact the Dean as a matter of urgency.

### **Recovering records affected by a disaster**

Assessing damage to records - Consider the following when assessing the damage caused to records:

- Determine what records are affected:
  - Are the records official or unofficial?
  - Are the records still required (consider administrative, financial, legal requirements and minimum retention requirements)?
  - What physical format are they (e.g. paper, video, tape, etc.)?
- Determine the extent of the damage:
  - Can the damage be repaired?
  - If wet, are they damp, only a little wet, or soaked?
- Determine where your area's records are listed
  - Does the area have a Recovery Priority List?
  - Is there an accessible copy of the Records Database (on the IT system)?

### **Post Recovery Review**

After the recovery of records has been successfully achieved, a strategic review should be taken on whether everything has gone to plan, all the records have indeed been recovered, whether there are any outstanding issues that need to be addressed. Depending on the level of the disaster, a meeting should be initiated chaired by the Dean, to review the following issues:

- An objective assessment of the disaster with a detailed outline of the timeline as well as its impact on the records-related
- The recovery operation – as to what was done by whom when
- What the current state of the records are – as to loss or damage



- Possible actions that can be taken to remedy any ongoing deficiencies in the state of the records
- Deficiencies in the entire recovery plan which need to be addressed
- Implementation action plan as a result of the meeting

Any post-recovery review documentation should be copied to EIT records.