RECORDS MANAGEMENT POLICY

Policy / Document Approval Body:	Academic Board
Date Created:	26 February 2010
Policy Custodian:	Dean of Engineering
Policy Contact:	Technology Manager
Location on EIT website:	https://www.eit.edu.au/about/policies-procedures/
Review Period:	Every Three Years
Revision No:	8
Date of Revision:	9 November 2023
Date Approved:	21 November 2023
Date Commenced:	22 January 2024

CONTENTS

1.0 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. This policy allows EIT to meet its business, legal, personal, and cultural obligations.

2.0 Scope

This policy extends to all EIT staff, both administrative and academic, who handle records (as defined below).

3.0 Overview

This policy document covers record keeping and management systems requirements, responsibilities, creation, management, and disposal of records. Other issues such as transfer of custody, security, access, details of student and staff files, and handling records when a disaster occurs are also covered.

4.0 Introduction

This policy establishes records management systems which support the objectives of EIT's Strategic Plan so that EIT shows excellence in management, staff, and staffing processes.

Record keeping strategies and practices are developed and managed by the Technology Manager, in consultation with the Dean, 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 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 tasks 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.

5.0 Record Keeping and Management Systems

EIT's record keeping 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 record keeping system is developed and managed by the Technology Manager, in consultation with the Dean, who provide ongoing support, development and training to organisational units, so that the EIT's legislative, business and community responsibilities are met.

EIT's record keeping systems manage paper-based and technology-dependent records and websites. EIT's corporate system includes paper-based and technology-dependent files of administrative, committee papers, staff and student records. Many of these are of enduring value because they capture EIT's decision-making processes.

6.0 Responsibilities

The Dean must ensure that EIT makes and keeps full and accurate records of its activities; and has regard for any relevant policy, standards, and guidelines about the making and keeping of public records.

Senior staff, such as the Deputy Dean, are responsible for ensuring that adequate records are captured and maintained for use by authorised personnel in the conduct of their business.

The Technology 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 Technology 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 Technology Manager manages records of enduring, permanent value which are no longer required for current administrative purposes. They provide 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 international privacy and data protection regulations where relevant and possible.

The Dean 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.

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 authorized disposal schedules.

7.0 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; and
- 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; and
- inadequate historical records of EIT.

8.0 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. 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.

Electronic backup routines for critical systems:

- Network Internal Drives:
  - IT Manager takes a backup every day;
  - VET and Higher Education; data is synchronized to Office 365 platforms to provide a secondary backup platform; and
  - Daily snapshots taken, and hard drives with the data are taken offsite every week.
- EIT/IDC Customer Facing Sites:
  - Server snapshots automatically taken every day with a 7-day retention period; and
  - Total system download is taken every month.
- Customer Relationship Management system:
  - Server snapshots automatically taken every day with a 7-day retention period; and
  - Total system download is taken every month.

- Learning Management System:
  - Server snapshots automatically taken every day with a 7-day retention period;
  - Total system download is taken every month; and
  - Completed courses are archived and downloaded following their completion.
- Student Management System:
  - Managed backups are undertaken by the provider of the SMS; and
  - CSV backups are downloaded and kept internally every week.

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.

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 will be responsible for clarifying this issue.

The 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.

9.0 Training

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

10.0 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 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 Technology Manager will be advised, and appropriate arrangements made to ensure that EIT's record keeping responsibilities are fulfilled.

The Technology 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.

11.0 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.

11.1 ICT Privacy and Security Measures

To ensure proper privacy and security measures are utilized surrounding digital and online student personal and private data, the following steps are taken:

- Data is backed up automatically at the relevant hosting provider's storage on a regular basis;
- Any lecturer and student online interfaces are password protected;
- All data transfers are made over SSL;
- Access restricted via Linux and Windows firewalls respectively and native hosting provider security/firewall;
- In case of breach, the following will be attempted:
    - Put system on lockdown;
    - Scan for vulnerabilities;
    - Assess and patch vulnerabilities;
    - Ensure all applications are up to date; and
    - Once cleared put system back online.
- System failure oversight mechanisms are implemented by means of backup recovery and alternative server switchover.

12.0 Access

It is expected that EIT's record keeping systems will provide timely and efficient access to and retrieval of records. Its 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 Technology 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. Remote access to EIT's systems requires password authentication. Privilege levels have been appropriately assigned to mitigate the impact of a breach if an account is compromised.

13.0 Donations of Non-EIT Records

EIT, on occasion, may receive records from external or non EIT courses. 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.

14.0 Email and Electronic Communication Records

Email (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), emails may be captured electronically into this system and managed as a record. All email messages should provide sufficient information so that the content is clear and that they can be properly classified into the relevant file.

15.0 Student files

The files of EIT students contain information that relates 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 management system (SMS), the student file may provide additional information to support the processes.

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

Completed student assessment items will be kept electronically for each student for a period of six (6) months from the date on which the assessment judgement for the student was made. However, students' marks and grades shall be kept electronically for a minimum of thirty (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 archived and stored in a secure manner. They include those aspects of a student record that contain the following information:

- Bank Account details and credit card details;
- Passport details
- Birth certificates

All records are subject to freedom of information requests.

16.0 Staff Files

An official EIT Staff File is established for all new 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 stored electronically in SharePoint and can only be accessed by the HR Manager and payroll. - All staff members are required to forward copies of any correspondence relating to staff employment activities of continuing staff

to the HR Manager via email only. 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;
- Appointment correspondence (both offer and acceptance);
- Records of employment (e.g., start and stop of work);
- Any contract amendmentInduction checklist;
- 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);
- 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 HR Manager in a confidential location.

Staff files are kept 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.

17.0 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 EIT and include:

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

The appropriate policy contact (such as the Accreditation and Compliance Manager) will manage the papers for committees appointed by the Governance Board or the Academic Board.

Board and Committee papers of EIT's organisational structure are of enduring value and must be transferred to the Technology Manager for permanent retention. When issues arise that have an immediate or potential bearing on EIT policies and procedures, the Accreditation and Compliance Manager should be notified so a review of the relevant policies and procedures can be facilitated.

As specified in the Policy Development and Review Process Guideline the approval date of any revisions to policies or procedures should be recorded in the policy directory.

18.0 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.

19.0 Audits

Besides informal audits, regular audits shall be conducted by the Technology 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.

20.0 Risk and Disaster Management Regarding Records

20.1 Introduction

Risk and Disaster Management as a general category is considered at a higher level within the organisation 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 unauthorized access or disclosure, which can:

- damage (or destroy) student records;
- damage (or destroy) staff records;
- undermine the effectiveness of EIT's operations;
- breach legal requirements;
- create difficulties in supporting EIT or stakeholders' rights; and
- 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 record-keeping 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 record keeping 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; and
- enable business units to take action to reduce the effects of a disaster which may affect their hard copy records.

The risk and disaster management section include:

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

20.2 Risk Management Programs for Records

The EIT Records Management Policy is in itself a risk management tool. The Records Management Program ensures sound record keeping 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; and
- premature destruction of records without appropriate approval or retention of records without documented reason.

20.3 Repository and Archive Management Program

EIT's archive repositories are managed by EIT's IT department. 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.

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

20.4 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 the destruction of records can be authorised.

EIT's destruction procedures are designed to prevent:

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

20.5 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 record keeping 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 record-keeping 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; and
- 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.

20.6 Preparing for a Disaster

To prepare for a disaster in advance and minimise the disruption it will cause, instructions on server management, maintenance, and start/stop procedures are saved on the server as well as paper copies stored in a securely locked storage space. In case of disaster, this information is accessible by pre-authorised staff, including the Dean, Deputy Dean, Technology manager, IT support staff, and selected Faculty.

All electronic details should be backed up on a continuous basis using the latest server technology and these materials are removed from the site at least once per week. This means that a working system can be set up on new computer hardware within (four) 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.

20.7 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 Technology Manager will be the key contact.

20.8 Responding to a Disaster Involving an Evacuation

The following actions should be taken by staff in response to a disaster affecting hard copy records 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 a senior member of staff (whoever is around at the time of the disaster); and
- If the effects of the disaster cannot be managed with in-house resources, the Emergency Management Team may bring in external disaster recovery specialists.

20.9 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 the 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; and
    - 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 Technology Manager. These lists should be developed and maintained as part of the disaster preparedness plan. Key record keeping 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.

20.10 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)?

20.11 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; and
- Implementation action plan as a result of the meeting.

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

21.0 Definitions

Please refer to the EIT Glossary that can be found here for all definitions used in this document.

22.0 Essential Supporting Documents

- AS ISO 15489 Records Management standard
- *"Retention requirements for completed student assessment items"* issued by ASQA 10 September 2022.
- "Compliance in Focus: Cyber Security" issued by TEQSA 8 May 2023

23.0 Related Documents

- Business Continuity and Disaster Recovery Plan.DS
- EIT Contingency and Succession Plan.DS
- EIT Facilities.DS
- EIT04 Accurate and Accessible Information Policy
- EIT07 Governance and Administration Policy
- EIT08 VET Regulator Cooperation & Legal Compliance
- Emergency and Critical Incident Policy & Procedure.DS
- Critical Incident Form
- Health and Wellbeing Policy and Procedure.DS
- Information Management and Security Policy and Procedure.DS
- Marketing and Promotion Policy and Procedure.DS
- Privacy Policy.DS
- Recruitment, Selection, Appointment and Induction Policy.HE
- Recruitment, Selection, Appointment and Induction Procedure.HE
- Risk Management Policy.DS
- Risk Management Register.DS
- Selection, Appointment and Induction Policy – Academic and Administration Staff.VET
- Selection, Appointment and Induction Procedure – Academic and Administration Staff.VET
- Work, Health and Safety Policy.DS

24.0 Related Legislation

The following legislation is relevant to this policy, however not all are mandatory for education providers:

- *Freedom of Information Act 1992 (WA)*
- *Higher Education Standards Framework (Threshold Standards) 2021 (Cwth.)*
- *Privacy Act 1988 (Cwth.)*
- *Public-Interest Disclosure Act 2003 (WA)*
- *Standards for Registered Training Organisations (RTOs) 2015 (Cwth.)*
- *Tertiary Education Quality and Standards Agency Act 2011 (Cwth.)*
- *Work Health and Safety Act 2011*

25.0 Accountabilities

The Academic Board is responsible for review and approval of this policy.

The policy is to be implemented via induction and training of staff and distribution to students and EIT's community via the website and other publications.