Safety and Security Policy - Students and Staff

<table>
<thead>
<tr>
<th>Policy/Document Approval Body:</th>
<th>Governance Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Created:</td>
<td>22 August 2012</td>
</tr>
<tr>
<td>Policy Custodian:</td>
<td>Dean of Engineering</td>
</tr>
<tr>
<td>Policy Contact:</td>
<td>Dean of Engineering</td>
</tr>
<tr>
<td>File Location:</td>
<td>W:\Data - ALL.Standard\Policies and Procedures\EIT Policies and Procedures</td>
</tr>
<tr>
<td>Review Period:</td>
<td>Three years</td>
</tr>
<tr>
<td>Revision No:</td>
<td>2</td>
</tr>
<tr>
<td>Date of Revision:</td>
<td>24 October 2012</td>
</tr>
</tbody>
</table>

Definitions:

**Accountable Person:** All management and supervisory staff, including those with responsibility for students, who assume responsibility for the health or welfare of any other person in a workplace by providing instruction, direction, assistance, advice or service.

**Cyber Bullying:** Cyber bullying is defined in legal glossaries as:
- actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm another or others.
- use of communication technologies for the intention of harming another person
- use of internet service and mobile technologies such as web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.

**Employee:** Any employee of the EIT.

**Home-based site:** Part of a dwelling that is remote from the EIT’s physical campus at West Perth where the employee will conduct their e-learning activities.
**Home-based work:** Regular performance of e-learning duties at the home-based site as agreed between the EIT and the employee.

**Occupational Health & Safety (“OH&S”) Considerations:**
Under the Workplace Health & Safety Act 1995 and 1998, an employer must ensure that employees have a safe working environment irrespective of whether they are working at the employer’s premises or working in a remote location.

**Working From Home Assessment Checklist:** The signed document outlining the conditions under which employees work from home on behalf of the EIT.

**Responsibilities:** In accordance with the Workplace Health & Safety Act 1995 to ensure that:
- employees of the EIT are made aware of the requirements of the Occupational Health & Safety (OH&S) guidelines.
- employees complete a checklist with regard to what is considered a safe and secure environment for the performance of their e-learning duties.
- all Working From Home Assessment Checklists are formally recorded on the employee’s personal file.

**Purpose:** The purpose of this policy is to set out the way the EIT intends to monitor health, safety and security issues with a view to the prevention of accident or injury to staff working at the EIT’s physical premises in West Perth, or at another place remote from that location, and students working in an online environment.

**Scope:** This policy applies to all EIT students, administrative and academic staff currently working for or enrolled with the EIT.

**Overview:** The EIT is committed to providing a safe and healthy place of work and study for all students and employees. This applies to all students of EIT, staff based at the EIT’s physical campus and staff engaged in e-learning activities generated from locations that are remote from the physical campus.

**Essential Supporting Documents:**
- Workplace Health & Safety Regulations 1998
- Australian/New Zealand Standard: 4442:1997 Office Desks. Standards Australia
1.0 SAFETY & SECURITY OF STAFF

1.1 Promoting Awareness of OH&S Considerations among Staff

The Policy Custodian, in consultation with the EIT’s Accountable Persons, will ensure that all OH&S guidelines are followed with regard to the EIT’s premises in West Perth in order that a safe and secure working environment is maintained for staff based at this location. As far as is practical, the EIT’s Accountable Persons will do what is possible to ensure that employees carrying out their work at remote e-learning sites are also made aware of OH&S guidelines and adhere to them. The EIT will not be responsible for any liability on the part of a third party who is not an employee at the home based work environment. All EIT employees will be encouraged by the Policy Custodian to consider all safety and security issues and ensure they work in accordance with OH&S requirements. To promote an awareness of OH&S considerations in relation to their learning environment, EIT Staff are referred to the following website in the EIT Student Handbook:

“How to Set Up an Ergonomically Correct Workstation”
http://www.wikihow.com/Set-Up-an-Ergonomically-Correct-Workstation

1.2 Office Accommodation

The Policy Custodian will ensure that the EIT maintains safe, well-maintained facilities and infrastructure appropriate to its scale, scope, location and mode of delivery. This includes appropriate work environments for employees based at the EIT’s premises in West Perth.

The Policy Custodian will oversee the planning, maintaining and updating of the EIT’s office space and systematically evaluate space requirements and other OH&S requirements based on current and projected space utilisation needs and assessments.

Factors to be considered in assigning space will include:

• The overall interests of the EIT.
- The suitability of present uses and possible future uses with anticipated or ongoing construction, renovation and planning of major space reallocations.
- The costs incurred by changing the use of space and how they will be borne.
- The effects of changing uses on employees.

1.3 Procedure with Regard to the Changing of Physical Facilities of the EIT
The Dean considers any changing space requirements or other OH&S requirements as they come to his attention. The Dean submits requests for changes to the Chair of the Governance Board. Requests are reviewed before final approval is given. In the event approval is denied, the Dean and any other persons responsible for the submission may resubmit a subsequent request in due course.

1.4 Equipment and Utilities Used at the Home-Based Site
The EIT and employees working at a remote location should identify the equipment required by these employees in order to undertake their work duties at the home-based site. The list should include items such as telephone, mobile telephone, computing equipment and stationary. This list will specify who owns each item and has responsibility for its maintenance and insurance. The final agreed list that is negotiated between the Accountable Person and the employee will be attached to the “EIT Working From Home Assessment Checklist” together with any drawings, photos, dimensions etc. that further explain OH&S considerations with regard to their workplace.

1.5 Security - Computer Network
The Accountable Person and the employee must ensure that arrangements are in place for the security of the computer network and that the employee whilst working from home will abide by the established security standards and guidelines of the EIT. All employees working at a remote location will ensure they have appropriate anti virus software on their computers. The EIT will ensure that the computers of all staff working at the EIT’s premises have appropriate anti virus security.

1.6 Contact Availability
Contact arrangements will be agreed between the employee and Accountable Person of the EIT. The employee’s home contact details will remain confidential and will not be provided to other people unless the employee has agreed in advance.

1.7 Information Technology
The EIT staff must use the authorised information systems or parts of the authorised system only for the purpose for which the authorisation was given. The EIT staff who have access to an information systems or part of an information system, shall not allow any unauthorised person access to that system for any reason.

The EIT staff must not access information which they are not authorised to access or use, and must not allow any other person access for any reason. Staff must
take all reasonable precautions, including password maintenance and file protection measures to prevent unauthorised access.

The EIT staff have an obligation to maintain the security and confidentiality of the information systems over which they have responsibility or control and that are owned, leased or used under licence or by agreement by the EIT.

1.8 Recordkeeping and Management Systems
The 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.

For further information on record keeping and Management Systems, please refer to the EIT Records Management Policy at:

2.0 SAFETY & SECURITY OF STUDENTS

2.1 Promoting Awareness of OH&S Considerations among Students
All EIT courses are delivered online rather than through the more conventional mode of teaching and learning where students attend a physical campus. Only in exceptional circumstances do students come to the EIT’s physical premises. The EIT encourages students to consciously consider the health and safety of the environment in which they participate in online education. To promote an awareness of OH&S considerations in relation to their learning environment, students are referred to the following website in the EIT Student Handbook:

“How to Set Up an Ergonomically Correct Workstation”
http://www.wikihow.com/Set-Up-an-Ergonomically-Correct-Workstation

2.2 Recordkeeping and Management Systems
The 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.

For further information on record keeping and Management Systems, please refer to the EIT Records Management Policy at:

2.3 Website Privacy
The EIT recognises and respects student privacy. When a student contacts EIT or purchases any of EIT products or services a record is created with the student’s contact information. The EIT treat this information with the highest standards of confidentiality and privacy. Personal student information will only be used for the purposes for which the student has disclosed it to EIT. The EIT will not disclose personal student information to any third party without the express consent of the student, unless required to do so by law. For
further information please refer to the EIT Website Privacy Statement at http://eit.edu.au/privacy

2.4 Cyber Bullying
The EIT supports the rights of all persons to work or study in an environment that is free from cyber bullying. The EIT is committed to the application of occupational health and safety, ethical behaviour and social justice.

The EIT supports the proactive strategies in place to educate staff and students about cyber bullying and harassment and the importance of the respect for diversity in work and study environments.

The EIT understands that educating staff and students about bullying and respect for diversity is a key strategy in preventing bullying from occurring.

The Internet is accessed by millions of people all over the world. While many Internet users are friendly, some may be malicious. Below are some ways to stay cyber-safe:

- Students should never share their Internet passwords with anyone.
- Students should never post or share their personal information online (this includes their full name, address, telephone number, names of family members or credit card numbers)
- Students should never meet anyone face-to-face whom they only know online.

Should a student experience cyber bullying, the following should be applied.

- Students are encouraged not to respond to cyber bullies.
- Students should never try to seek revenge on a cyber bully.
- Students should report any incidents of cyber bullying to a relevant EIT staff member who will manage the incident in the appropriate manner. Students are to keep a record of cyber bullying incidents and to provide the EIT staff member with the electronic correspondence the cyber bullying relates to.

2.5 Student Responsibility for Internet Safety and Security
It is the responsibility of students at EIT to ensure they have adequate internet safety and security and to protect their computers. The following list contains some simple precautions students can take to protect themselves.

1. Install anti-virus and other security software, such as anti-spyware and anti-spam software. Use and update this software regularly.
2. Regularly download and install the latest security patches for your computer software, including your web-browser. Use automatic software security updates where possible.
3. Use a firewall and make sure it is turned on. Firewalls help prevent unauthorised access to, and communications from, your computer.
4. Delete suspect emails immediately. This may be a scam or contain a virus so don't open these emails.
5. Don't click on links in suspect emails. Visiting websites through clicking on links in suspect emails may result in malware (malicious software), such as a ‘trojan’, being downloaded to your computer. This is a commonly used and effective means of compromising your computer.

6. Only open an attachment to an email where the sender and the contents of the attachment are known to you.

7. Don't download files or applications from suspect websites. The file or application could be malware. Sometimes the malware may even be falsely represented as e-security software designed to protect you.

8. Use long and random passwords for any application that provides access to your personal identity information, including logging onto your computer. Don't use dictionary words as a password. Ideally, the password should be eight or more characters in length. Change passwords regularly.

9. Use a limited permission account for browsing the web, creating documents, reading email, and playing games. If your operating system allows you to create a limited permission account, this can prevent malicious code from being installed onto your computer. A ‘limited permission' account is an account that does not have ‘Administrator' status.