EASTERN INSTITUTE OF TECHNOLOGY
TE AHO A MĀUI

Privacy – Policy QA190

PURPOSE

The purpose of this policy is to ensure that any personal information collected or held by EIT is managed in compliance with legislation, specifically the Privacy Act 2020 and its associated regulations, and the privacy promises made to the person(s) to whom the information relates.

SCOPE

This policy applies to all EIT staff members (whether permanent, temporary or casual), and any members of EIT Board, committee members, committee appointees, contractors, subcontractors, alumni, or students who are explicitly permitted access to personal information held by EIT.

POLICY BACKGROUND

EIT collects and processes personal information about learners, graduates, donors, staff, research participants, prospective staff or students and any individuals who visit in person or digitally. EIT has a duty to ensure that any 'individual concerned' knows why their personal information is being collected, that the information will be used responsibly and treated with care and respect.

The legislation identifies key **information privacy principles** which inform EIT's approach to managing personal information:

1. Purpose of Collection
2. Source
3. Collection
4. Manner of Collection
5. Security of Information
6. Access
7. Correction
8. Accuracy
9. Retention
10. Limits on Use
11. Limits on Disclosure
12. Sharing Information Overseas
13. Unique Identifiers

DEFINITIONS

Individual(s) concerned means any natural person or persons about whom EIT collects and holds personal information and includes students, staff members (current and former), contractors, alumni and friends, donors, and visitors to any of EIT's locations. *Note: This is a global term which we are using to ensure consistency. The Privacy Act 2020 uses the term "individual concerned".*

Lawful purpose means a purpose that is directly connected with any of EIT's lawful functions, and includes, but is not limited to considering applications for admission to, or employment with EIT, administering programmes of study; managing staff and ensuring the health, safety and wellbeing of students and staff members; and meeting EIT's reporting requirements.

Personal information means any information, whether electronic or hard copy, about an identifiable individual concerned, and includes but is not limited to contact, demographic, health and academic information (including course results), CCTV footage, staff information, emails and other correspondence, and opinions about the individual(s) concerned. Identifiable information does not just mean information naming the individual(s), but also includes information that could be reasonably linked to the individual(s) concerned.

Privacy breach means a situation when personal information is lost, stolen, accessed or provided to a third party without permission. Further information on the management of privacy breaches is in the Procedure PA190.

CONSULTATION PROCESS

Executive Team, Director Information Technology and Facilities, Director Information Management and Learning Services, Managers, Students (through the Students' Association Younited), EIT Staff.

QUALITY OUTCOMES

The key **Information Privacy Principles** (IPPs) and other requirements in the Privacy Act 2020 should be adhered to in as much as it relates to work or study.

OUTPUT STANDARDS

EIT staff as outlined in Scope must:

1. Understand and comply with the EIT Privacy policy and procedures. There should be awareness of the following aspects of Privacy Act 2020, as outlined in the Privacy Brochure:
    - Using Personal Information at EIT
    - Types of common breaches
    - Handling Personal Information at EIT
    - Storage of Personal Information
    - Examples of Misuse
2. Actively participate in any privacy training provided by EIT, and
3. Keep managers and/or the Privacy Officer informed of any privacy breaches, near misses or other privacy issues.
4. Respond to information requests from individuals by providing them with their information (if they are confident of the person's identity and that it is appropriate to share that information) or otherwise referring the request to a Manager or the Privacy Officer.

Managers must:

1. Support staff to understand and comply with this policy and participate in any privacy training provided by EIT, and
2. Ensure privacy breaches, near misses and other privacy issues are identified and managed in accordance with the EIT Policy and Procedure.
3. Respond to information requests from individuals by providing them with their information (if they are confident of the person's ID and that it is appropriate to share that information) or otherwise referring the request to the Privacy Officer.

The Privacy Officer(s) will:

1. Support understanding and compliance with EIT Privacy policy and procedures, including by maintaining and developing relevant procedures.
2. Engage and assist with Privacy Impact Assessments and encourage privacy by design in new projects or processes.
3. Advise on information requests/corrections and processes.
4. Assist with the management of privacy breaches, near misses and other privacy issues.
5. Manage privacy complaints from individual(s) concerned.
6. Liaise with third parties in respect of privacy matters, including the Privacy Commissioner or other relevant regulators and individual(s) concerned.

7. Be well-informed of changes to the privacy laws and regulations which can impact on how EIT operates.
8. Ensure EIT Privacy Statements or other key information provided are up-to-date and fit for purpose.
9. Ensure regular training is made available to staff and support documents are readily available.

COMPLIANCE STANDARDS

Information Privacy Principles (IPP)

1. Purpose of Collection

Personal information will only be collected for a lawful purpose connected with a function of EIT and the collection must be necessary for that purpose. Information should only be collected in an identifying form if that is necessary for carrying out a lawful purpose.

2. Source

Personal information must normally be collected from the individual concerned, not a third party. Exceptions sometimes apply and are outlined in IPP 2 of the Privacy Act 2020.

3. Information on Collection

At the point of collection, the individual must be aware of key details, including what will happen to their information, and that they have the right to access their information and to seek corrections. See IPP 3 for more information.

4. Manner of Collection

Information must be collected lawfully, fairly and reasonably.

5. Security of Information

All reasonable steps must be taken to protect the safety and integrity of personal information held by EIT.

6. Access

An individual is entitled to access their own information held by EIT, where that information can readily be retrieved. There is a time-frame and process for responding to requests for information that EIT must follow.

7. Correction

An individual may request correction of any information held about them by EIT. There is a time-frame and process for responding to requests for corrections that EIT must follow.

8. Accuracy

Reasonable steps must be taken to ensure that before use or disclosure, information is accurate, up to date, complete, relevant and not misleading.

9. Retention

EIT keeps information only for as long as necessary for the purposes for which the information may lawfully be used.

10. Limits on Use

Information may only be used for purposes for which it was collected or if another exception applies (see IPP 10 in the Privacy Act 2020).

11. Limits on Disclosure

Information may not be disclosed except for the original purpose for which it was obtained, or with authorisation from the person, or in specific other circumstances (see IPP 11 in the Privacy Act 2020).

12. Sharing information overseas

1. The EIT Privacy Officer will guide staff on responding to any requests for overseas information disclosures, due to the restrictions on how and when EIT can disclose personal information overseas.
2. The EIT Privacy Officer may need to consult with legal advisors on complex overseas information requests.

13. Unique Identifiers

Unique identifiers may only be used when necessary for efficiency. Another agency’s unique identifier should not be used.

REPORTING STANDARDS

1. Anyone who observes a privacy near miss, or causes or discovers a privacy breach must *as soon as practicable* report the breach, as per the Procedure PA190.
2. The Privacy Officer must notify privacy breaches to the Chief Executive’s Office within 24 hours of becoming aware of the breach.
3. Privacy breaches that have caused or are likely to cause anyone serious harm must be notified to the **Privacy Commissioner** *as soon as practicable* after EIT has become aware of the privacy breach. (Privacy Act 2020 requirement)
4. Any findings from Privacy Breach investigations must be reported to the Chief Executive and the Privacy Officer.
5. Regular summary reporting of near misses, breaches and resulting outcomes will be undertaken.

Document information – Office use only	
Document Name	Privacy
Document Number	QA190
Executive	Executive Director, Student and Academic Services
Owner	Executive Director, Student and Academic Services
Developer	Privacy Officer
Review Frequency	12
Last Review	4/10/2021
Next Review	4/10/2022
Related Items	Click here for Related Documents (available only on Staffnet) QH100 Staff Code of Conduct
Version history	Format updated May 2018