Privacy Policy

Policy Category	**Policy**/guideline/procedure/rules		
Review	3 years from date of Approval		
Policy Code	GP006		
Contacts	policy@top.edu.au		
Version	Approval Authority	Approval Date	Commencement Date
2019.04	Executive Team	19 April 2019	19 April 2019

1. Purpose

The Institute is committed to providing all stakeholders with the highest levels of professional service. The purpose of this Privacy Policy is to communicate to you how we manage, collect, deal with, protect and allow access to personal information in accordance with the *Privacy Act 1988 (Cth) (the Privacy Act)*, the *Australian Privacy Principles (the APPs)*, the *Health Records and Information Privacy Act 2002* (HRIPA) and other relevant privacy laws, including but not limited to regulations, statutory guidelines, codes of practice and privacy directions. We understand the importance placed on the privacy of your personal information. The Institute will endeavour to make you aware of the contents of this Privacy Policy before or as soon as reasonably practicable after collecting any personal information about you.

2. Scope

This Privacy Policy applies to our management of the personal information of our students, clients, customers, suppliers and prospective employees. This Privacy Policy does not apply to our acts and practices which relate directly to the employee records of our current and former employees.

The policy forms part of all Institute agreements, contracts and business practices which involve collection and/or management of personal information.

3. Principles

<u>Why do we collect, hold, use and disclose personal information?</u>
We collect, hold, use and disclose personal information for the following purposes:

- to process applications for study and work; and
- as is reasonably necessary and convenient for our business' functions and activities.

Unless otherwise provided by law, we will not collect, hold, use or disclose sensitive information without your consent.
If you would like to access any of our services on an anonymous basis or by using a pseudonym, please tell us. However, we will require you to identify yourself if:

- we are required by law to deal with individuals who have identified themselves; or
- it is impracticable for us to deal with you if you do not identify yourself or elect to use a pseudonym.

Please be aware that your request to be anonymous or to use a pseudonym may affect our ability to provide you with the requested goods and/or services.

What kind of personal information do we collect and use?

The nature and extent of personal information that we collect varies depending on your particular interaction with us and the nature of our functions and activities.

Personal information that we commonly collect, hold, use and disclose could include your name, position, date of birth, current address, facsimile numbers, email address, telephone numbers, next of kin, tax file number, education details, Australian Business Number, bank details, business references, financial details, details about your business, drivers licence number and preferred means of contact, professional and academic credentials, hobbies and interests.

How do we collect and hold personal information?

Where possible, we will collect personal information directly from you. We collect information through various means, including interviews, appointments, forms, surveys, applications and questionnaires (whether in hardcopy or electronic format, including information submitted via our website or other electronic means). If you feel that the information that we are requesting, either on our forms or in our discussions with you, is not information that you wish to provide, please feel free to raise this with us.

In some situations we may also obtain personal information about you from a third party source. If we collect information about you in this way, we will take reasonable steps to contact you and ensure that you are aware of the purposes for which we are collecting your personal information and the organisations to which we may disclose your information, subject to any exceptions under the *Privacy Act.*

If we receive unsolicited personal information about you that we could not have collected in accordance with this Privacy Policy and the *Privacy Act,* we will within a reasonable period, destroy or de-identify such information received.

Our internet service provider may record details of visits to our site and when visiting our site your visit may be logged and the following information collected:

- the visitor's server address, domain name and browser type;
- the date and time of the visit to the site;
- the pages accessed and the documents downloaded;
- the previous website visited;
- the user's operating system; and
- the links followed from other sites to get to the current site.

The information listed above will only be used by us internally for statistical and research purposes.

When do we use and disclose your personal information?

We will only use and disclose your personal information:

- if we get your consent; or
- for purposes which are related to the purposes for which the information was collected,
- in accordance with this Privacy Policy and the Privacy Act.

For the purposes referred to in this Privacy Policy, we may disclose your personal information to other

parties including:

- your referees;
- your former employers;
- your education providers;
- credit agencies;
- our professional advisors, including our accountants, auditors and lawyers;
- our Related Entities and Related Bodies Corporate (as those terms are defined in the *Corporations Act 2001* (Cth)); and
- our employees, contractors and suppliers;
- Professional membership agencies;
- Professional accreditation authorities;
- Disclosure to government agencies with responsibility for administering and regulating education providers in Australia, such as Tertiary Quality Standards Agency (TEQSA), and the Tuition Protection Services (TPS) and disclosure to government agencies with responsibility for administering immigration and student visa arrangements (including disclosure of suspected breaches of student visa conditions).

We will only use or disclose your personal information for the purposes of direct marketing if:

- we collected the information from you;
- it is reasonable in the circumstances to expect that we would use or disclose the information for direct marketing purposes;
- we provide you with a simple means to 'opt-out' of direct marketing communications from us; and
- you have not elected to 'opt-out' from receiving such direct marketing communications from us.

Do we send information overseas?

It is likely that we will disclose personal information to overseas recipients and it is not practicable for us to specify the countries in which overseas recipients of personal information are located.

If we disclose your personal information to overseas recipients, we will take reasonable steps to ensure that such recipients do not breach the Privacy Act and the APPs unless:

- we believe that the overseas recipient is subject to a law that has the same effect of protecting personal information in a way that, overall, is at least substantially similar to the way in which the Privacy Act and the APPs protect personal information and there are mechanisms available for you to access to take action to enforce that protection of law; or
- we obtain your express consent to the disclosure of personal information to overseas recipients.

Access to and correction of your personal information

You have a right to access your personal information.

We are not obliged to allow access to your personal information if:

- we reasonably believe that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;

3

- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between you and THE INSTITUTE and would not ordinarily be accessible by the discovery process in such proceedings;
- giving access would reveal our intentions in relation to negotiations with you in a way that would prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order;
- we have reason to suspect that unlawful activity, or misconduct of a serious nature relating to our functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- giving access would reveal internal evaluative information in connection with a commercially sensitive decision-making process.

We will also take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading if:

- we are satisfied the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to a purpose for which it is held; or
- you request us to correct the information.

If you make a request for access to or correction of personal information, we will:

- respond to your request within a reasonable period; and
- if reasonable and practicable, give access to or correct the information in the manner requested.

If we refuse to give access to the personal information because of an exception or in the manner requested by you, we will give you a written notice that sets out at a minimum:

- our reasons for the refusal (to the extent it is reasonable to do so); and
- the mechanisms available to complain about the refusal.

If we refuse a request to correct personal information, we will:

- give you a written notice setting out the reasons for the refusal and how you may make a complaint; and
- take reasonable steps to associate a statement with personal information it refuses to correct;

We reserve the right to charge you reasonable expenses for providing access or making a correction to personal information, for example, a fee for photocopying any information requested by you. If we charge you for giving access or making a correction to your personal information, such charges must:

- not be excessive; and
- not apply to the making of the request for access or correction to personal information.

Nothing in this Privacy Policy replaces other informal or legal procedures by which an individual can be provided with access to or to correct personal information.

<u>Integrity of your personal information</u>

We will take reasonable steps to:

- ensure that the personal information that we collect is accurate, up to date and complete;

4

- ensure that the personal information that we hold, use or disclose is, with regard to the relevant purpose, accurate, up to date, complete and relevant; and
- secure your personal information.

We will take reasonable steps to protect personal information from:
- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

We will take reasonable steps to destroy or de-identify personal information that we hold if we no longer need the information for the primary purpose for which the information was collected and we are not otherwise required by law to retain the information.

Anonymity, Identifiers and Transfer of Health Information Outside NSW

In relation to health information, we will:
- provide individuals with the option of receiving health services anonymously; and/or
- assign a unique identification number to an individual,
- where it is reasonably practicable and lawful in the circumstances and it does not negatively affect the functions of TOP.

We will transfer health information outside New South Wales or to a Commonwealth agency, in limited circumstances, including where the recipient of the health information is subject to principles that are substantially similar to NSW privacy principles, the individual has provided consent or the transfer is necessary for the performance of a contract between TOP and a third party.

Further information concerning anonymity, identifiers and the transfer of health information outside NSW can be obtained from the details listed below.

Complaints

Individuals may make a complaint if they believe the Institute has mishandled their personal information.

The following must be reported to the Privacy Officer (listed below):
- concerns that the personal information contained in a record of a client,
- stakeholder's may have been mishandled;
- any complaints/allegations about a breach of privacy;
- all privacy-related matters referred from the Privacy Commissioner within the Office of the Australian Information Commissioner.

Personal information security breaches can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harm to individuals, agencies and organisations. Consequently, there is no single way of responding to a personal information security breach. Each breach will need to be dealt with on a case-by-case basis. All complaints and alleged breaches will be investigated by an independent privacy officer and the complainant will be advised of the outcome.

The Institute is committed to a quick resolution of all complaints.

You may also make a complaint directly to the Office of the Australian Information Commissioner (OAIC) online, by mail, fax or email. Please visit the OAIC website at http://www.oaic.gov.au/privacy/making-a-privacy-complaint for more information.

How to contact us

If you would like more information on privacy or have any questions in relation to this policy please email: policy@top.edu.au

Roles and Responsibilities

The Institute Privacy Officer is responsible for the Institute's overall compliance with its privacy obligations.

The Institute's Privacy Officers are responsible for:

- providing privacy advice and education to staff;
- responding to enquiries or complaints from individuals on privacy matters;
- implementing and maintaining this Privacy Policy, the Privacy Management Plan and TOP's privacy policy.

The Human Resources Division is responsible for the central management of staff information;

The Student Services Division is responsible for the central management of student information;

All staff are responsible for complying with the Institute's privacy obligations and practices as specified in this Privacy Policy and any of the Institute's codes of conduct or otherwise when managing information provided to, or collected by the Institute. This includes attending training or completing online privacy training as required.

4. Change and Version Control

Historical Version	Approved by	Approval Date
2013.12	Executive Team	20 December 2013
2018.08	Executive Team	17 August 2018
2019.04	Executive Team	19 April 2019

6