

Illawarra >> ITeC <<

Privacy Policy & Procedure

v004 – 13 July 2021

Document Title	Privacy Policy and Procedure
Operational Area	Administration
Date Created	22/06/2015
Reviewed by	Compliance Officer
Revision Date	13/07/21
Revision Number	004
Approved by	CEO

Introduction

It is a legislative requirement that client privacy be maintained at all times. In addition, Illawarra ITeC respects the privacy of staff and students and strives at all times to ensure that the level of privacy protection achieved through its operations is the highest possible.

Purpose

The *Privacy Policy and Procedure* has been implemented to ensure that Illawarra ITeC complies with its privacy obligations at all times.

Scope

The *Privacy Policy and Procedure* applies to the entire operations of Illawarra ITeC at all times.

Responsibilities

This policy and procedure are the responsibility of the Chief Executive Officer.

Definitions

No special definitions apply to this policy and procedure.

Alignment

The Illawarra ITeC complies with:
<ul style="list-style-type: none"> The Standards for Registered Training Organisations (RTOs) 2015: Compilation (3), 1 July 2019, including the clauses related to compliance and reporting (clauses 8.5 and 8.6) and providing requested information to the Australian Skills Quality Authority (ASQA) (clauses 8.1 and 8.2).
<ul style="list-style-type: none"> Higher Education Support Act 2003: Compilation (79), 24 June 2021
<ul style="list-style-type: none"> Australian Privacy Principles 12 March 2014
<ul style="list-style-type: none"> Privacy Amendment (Enhancing Privacy Protection) Act 2012: Compilation (1) 12 March 2014
<ul style="list-style-type: none"> Privacy Act 1988: Compilation (87), 17 June 2021
<ul style="list-style-type: none"> Student Identifiers Act 2014: Compilation (6), 1 January 2021
<ul style="list-style-type: none"> National Vocational Education and Training Regulator Act 2011 (NVR ACT): Compilation (18), 1 January 2021

Definitions

Personal and sensitive information

Under the Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act 2012 (s6(1)), personal and sensitive information is defined as follows:

Personal information: “information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.”

Sensitive information: “(a) information or an opinion about an individual's: (i) racial or ethnic origin, or (ii) political opinions, or (iii) membership of a political association, or (iv) religious beliefs or affiliations, or (v) philosophical beliefs, or (vi) membership of a professional or trade association, or (vii) membership of a trade union, or (viii) sexual preferences or practices, or (ix) criminal record, that is also personal and sensitive information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purposes of automated biometric verification or biometric identification; or (e) biometric templates”.

Australian Privacy Principles (APPs)

The Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act 1988 (Privacy Act), outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal and sensitive information.

While the APPs are not prescriptive, each APP entity needs to consider how the principles apply to its own situation. The principles cover:

- the open and transparent management of personal and sensitive information including having a privacy policy
- an individual having the option of transacting anonymously or using a pseudonym where practicable
- the collection of solicited personal and sensitive information and receipt of unsolicited personal and sensitive information including giving notice about collection
- how personal and sensitive information can be used and disclosed (including overseas)
- maintaining the quality of personal and sensitive information
- keeping personal and sensitive information secure
- right for individuals to access and correct their personal and sensitive information

Policy Statement

Privacy

The Chief Executive Officer of Illawarra ITeC must:

- Ensure that only authorised employees and learners have access to learner records.
- Retain and archives student records for a period of 30 years and transfer records consistent with State or Territory registering body requirements. Upon written request, students will have timely access to current and accurate records and the right to review and correct information if required.
- Evidence of participation in training and assessment activities will be maintained on the Illawarra ITeC computer network to meet the provisions of Legislative and Commonwealth contracts.
- Ensure a record of learner requests for access to personal records is maintained.
- Ensure that only authorised employees have access to employee records.
- Ensure that only authorised employees have access to stakeholder's confidential information.
- Restrict third party access to learners' or employee's personal records except as required by legislation or with the express written permission of the learner and/or their parent or guardian where relevant; and
- Comply with our legal requirements including the requirements of the Australian Privacy Principles set out in the Privacy Act 1988 and Clause 23 of Schedule 1A of the Higher Education Support Act 2003 in relation to the collection of information relating to all students and the Student Identifiers Act 2014.

Procedure

Personal and sensitive information

The Chief Executive Officer of Illawarra ITeC must:

- Ensure that personal and sensitive information is managed in an open and transparent way
- Not collect personal and sensitive information by unlawful or unfair means.
- If the collection of the information is authorised or required by or under law advise the parties of this fact, and with whom it will be shared.
- Confirm that only authorised employee enters learner personal and sensitive information accurately.
- Ensure that such information is stored securely against unauthorised access, use, modification or disclosure, and against other misuse, and loss.
- Ensure that employees update learner personal records within seven (7) days when their personal and sensitive information changes or when a request has been received in writing by the learner requesting their information be changed
- Confirm that authorised employees enter employee personal and sensitive information accurately or when a request has been received in writing by the employee requesting their information be changed.
- Ensure that employees update employee personal records when their personal and sensitive information changes.
- Confirm that authorised employees enter stakeholder information accurately.
- Ensure that such information is secure from unauthorised access; and
- Ensure that employees update stakeholder information when their information changes.

Collection of personal and sensitive information

The Chief Executive Officer of Illawarra ITeC

Must ensure learners are provided control over their personal and sensitive information.

In general, learners can visit our web site without providing us with any personal and sensitive information. However, there are instances where we must have learner personal and sensitive information for us to grant you an access to our protected and secured sites that may be used from time to time. This information may include registration data (your name, address, email address, phone number, title, etc.), information request data and response data ("User Information"). When you receive your confirmation email or when you receive any email from the list server, you will be given instructions on how to remove yourself from the list.

Personal and sensitive information privacy

The Chief Executive Officer of Illawarra ITeC:

Must ensure learner personal and sensitive information and privacy upon enrolment:

Most personal and sensitive information is provided to the Illawarra ITeC by students enrolling in a course by a paper-based Enrolment Form. Personal and sensitive information is also collected when a student or client completes a survey, questionnaire, or application form, and when prospective students and clients make enquiries about our services.

Generally, you are not obligated to provide any information requested by Illawarra ITeC that you do not wish to provide, except where it is needed by Illawarra ITeC to facilitate your enrolment and other compliance obligations. It is impracticable for Illawarra ITeC to deal with individuals who have not identified themselves or who use a pseudonym for enrolments purposes.

If you choose to apply to enrol into an accredited course with Illawarra ITeC then you must provide the personal and statistical information requested on the Enrolment Form. If you do not provide this information accurately, including your official name and matching data such as your date of birth, your enrolment cannot proceed and any enrolment fees will be refunded, less the Administration Fee.

You must also provide Illawarra ITeC with your unique government related Student Identifier which matches your official name and your date of birth. If a matching USI is not provided, you cannot be issued a Statement of Attainment or Testamur, and your enrolment may be cancelled with any applicable fee refund being subject to the Administration Fee.

If you are applying to enrol into a non-accredited course, you will need to provide your official name and other suitable matching data such as your date of birth. If you are unable to provide this information, your application to enrol cannot proceed and your course fees will be refunded, less the Administration Fee.

Sufficient information / documentation referred to above is needed to verify your identify satisfactorily. This is because, as a provider of nationally recognised qualifications, Illawarra ITeC has obligations to determine your identity, eligibility to any funded courses and obtain appropriate contact details to enable the provision of our student support services, and in respect to non-accredited courses to issue a Statement of Participation.

Direct Marketing - Controlling your personal and sensitive information

The Chief Executive Officer of Illawarra ITeC must:

Provide individuals with the option of choosing to restrict the collection or use of your personal and sensitive information in the following ways:

- Whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used for direct marketing purposes; and
- If you have previously agreed to us using your personal and sensitive information for direct marketing purposes, you may change your mind at any time by emailing us at itec@illawarraitec.edu.au.

Use or disclosure of your information

The Chief Executive Officer of Illawarra ITeC must:

Advise individuals on the use and disclosure of personal and sensitive information:

We may disclose personal and sensitive information:

- for the purpose of providing services to meet the provisions of government contractual requirements.
- for the purpose of meeting an obligation under government contractual requirements.
- to verify compliance with the agreement between Illawarra ITeC and your employer or job active provider, to keep track of the domains from which people visit us, to better serve you and your employer or job active provider, or to simply contact you either electronically or otherwise.
- to credit reporting agencies and courts, tribunals, regulatory authorities where customers fail to pay for services provided by us to them.
- to courts, tribunals, regulatory authorities, and law enforcement officers as required by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights and
- Illawarra ITeC does not disclose personal and sensitive information to third parties or overseas entities.

Data Security, records, and staff training

The Chief Executive Officer of Illawarra ITeC must:

- Keep all personal or stakeholder records in a secure location (both physical and electronic); and
- Keep backups in a secure location.
- Protect the personal and sensitive information which it holds from misuse, loss or unauthorised access, modification or disclosure by various means including firewalls, virus protection, strong password access, and secure servers.
- Maintain procedural documents setting out:
 - the nature of the records of personal and sensitive information kept.
 - the purpose for which each type of record is kept.
 - the classes of individuals about whom records are kept.
 - the period for which each type of record is kept.
 - the persons who are entitled to have access to personal and sensitive information contained in the records and the conditions under which they are entitled to have that access; and

- the steps that should be taken by persons wishing to obtain access to that information.
- Ensure that their staffs are suitably trained in relation to Privacy laws and the Illawarra ITeC obligations, Policy, and procedures.
- Ensure any hard copy records that are no longer required are shredded in-house or securely destroyed using a reputable document security destruction facility.

Cookies and web beacons

The Chief Executive Officer of Illawarra ITeC must:

Disclose to third parties unsolicited information and the collection of personal and sensitive information:

We may use cookies on our website from time to time. Cookies are text files placed in your computer's browser to store your preferences. Cookies, by themselves, do not tell us your e-mail address or other personally identifiable information. However, once you choose to furnish the Site with personally identifiable information, this information may be linked to the data stored in the cookie.

We may use web beacons on this Site from time to time. Web beacons or clear .gifs are small pieces of code placed on a web page to monitor the behaviour and collect data about the visitors viewing a web page. For example, web beacons can be used to count the users who visit A web page or to deliver a cookie to the browser of a visitor viewing that page.

Links to other websites

The Chief Executive Officer of Illawarra ITeC must:

Disclose that our website may contain links to other websites of interest. Illawarra ITeC web site provides links to other third-party web sites. Even if the third party is affiliated with Illawarra ITeC through a business partnership or otherwise, Illawarra ITeC is not responsible for the privacy policies or practices or the content of such external links. These links are provided to you for convenience purposes only and you access them at your own risk.

Web-based Meeting Portals

The Illawarra ITeC uses web-based meeting portals for face-to-face online meetings between students and their trainer/assessor. These webinars may be recorded and stored on Illawarra ITeC servers as they form evidence of student participation and student learning.

Web-based privacy policy

The following privacy policy is located on <https://zoom.us/privacy>.

Privacy is an extremely important topic, and we want you to know that at Zoom, we take it very seriously. Here are the facts about user privacy as it relates to Zoom and your use of our services:

- We do not sell your personal data. Whether you are a business or a school or an individual user, we do not sell your data.
- Your meetings are yours. We do not monitor them or even store them after your meeting is done unless we are requested to record and store them by the meeting host. We alert participants via both audio and video when they join meetings if the host is recording a meeting, and participants have the option to leave the meeting.
- When the meeting is recorded, it is, at the host's choice, stored either locally on the host's machine or in our Zoom cloud. We have robust and validated access controls to prevent unauthorized access to meeting recordings saved to the Zoom cloud.
- Zoom collects only the user data that is required to provide you Zoom services. This includes technical and operational support and service improvement. For example, we collect information such as a user's IP address and OS and device details to deliver the best possible Zoom experience to you regardless of how and from where you join.
- We do not use data we obtain from your use of our services, including your meetings, for any advertising. We do use data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com. You have control over your own cookie settings when visiting our marketing websites.
- We are particularly focused on protecting the privacy of K-12 users. Both Zoom's Privacy Policy (attached) and Zoom's K-12 Schools & Districts Privacy Policy are designed to reflect our compliance with the requirements of the Children's Online Privacy Protection Act (COPPA), the Federal Education Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA), and other applicable laws.

Archiving

The Chief Executive Officer of Illawarra ITeC must ensure that all personal and stakeholder records are archived in a secure location when no longer current.

Monitoring and Improvement

All practices for Privacy are monitored by the Chief Executive Officer of Illawarra ITeC and areas for improvement identified and acted upon (See Continuous Improvement Policy)

Amendments to this policy

This policy may be amended from time to time. Your continued use of our website and provision of personal and sensitive information following any such amendments will be deemed to be confirmation that you accept those amendments.

Related Documents

Continuous Improvement Policy