

PRIVACY POLICY

PURPOSE

Industrylink Training Pty Ltd is committed to the appropriate and lawful management of personal information, and in particular to compliance of, and respect of the privacy of personal information. We are committed to safeguarding the privacy of our clients; in this policy we set out how Industrylink collects and manages personal information; and how it will comply with the current Australian Privacy Principles (APPs).

Commencing in March 2014, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 changed the Privacy Act 1988 (Privacy Act). The Privacy Regulation 2013 also commenced in March 2014. The Privacy Act now includes a set of 13 new harmonised privacy principles that regulate the handling of personal information in the Government and private sector. These principles are called the Australian Privacy Principles. They replace both the Information Privacy Principles that applied to Australian Government agencies and the National Privacy Principles that applied to some private sector organisations.

SCOPE

This policy applies to all personal information collected, held, used or disclosed by Industrylink Training, and must be complied with by all staff, students, employers and other stakeholders of Industrylink Training Pty Ltd. This applies to any information collected by any means (electronic, verbal or in writing).

THE 13 AAPs (EFFECTIVE AS AT MARCH 2014)

Australian Privacy Principle 1:	open and transparent management of personal information
Australian Privacy Principle 2:	anonymity and pseudonymity - Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter
Australian Privacy Principle 3:	collection of solicited personal information - the entity must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.
Australian Privacy Principle 4:	dealing with unsolicited personal information - if an entity receives personal information; and did not solicit the information; the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

Australian Privacy Principle 5:	notification of the collection of personal information - the entity must take steps to notify the individual that they collect personal information, the purposes for which they collect the personal information, and the main consequences (if any) for the individual if all or some of the personal information is not collected by the entity.
Australian Privacy Principle 6:	use or disclosure of personal information - If an entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: the individual has consented to the use or disclosure of the information.
Australian Privacy Principle 7:	direct marketing - If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.
Australian Privacy Principle 8:	cross-border disclosure of personal information
Australian Privacy Principle 9:	adoption of government related identifiers - An organisation must not adopt a government related identifier of an individual as its own identifier of the individual
Australian Privacy Principle 10:	quality of personal information -An entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date, relevant and complete.
Australian Privacy Principle 11:	security of personal information - If an entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: from misuse, interference and loss; and from unauthorised access, modification or disclosure.
Australian Privacy Principle 12:	access to personal information - If an entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.
Australian Privacy Principle 13:	correction of personal information – If an entity holds personal information about an individual and the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests the entity to correct the information, that they do so in a timely manner.

COLLECTING PERSONAL INFORMATION

Industrylink Training may collect, store and use the following kinds of personal information:

- Information that a student provides when completing an enrolment form such as: name, address, postal address, gender, contact phone numbers, date of birth, next of kin details, educational details, employment details. This information is necessary for registering a student into a Nationally Recognised Qualification or short course.
- Alternative information from an enrolment form, such as: information about language and cultural diversity, disabilities, prior levels of study and reasons for study. This information is collected and provided to State and

Commonwealth agencies and research organisations as a part of the regulatory licensing of being a Registered Training Organisation.

- Contact information such as postal and e-mail addresses and telephone numbers. This is to ensure we have a fast way of communicating with our clients, students and other stakeholders.
- Information relating to any purchases a business may make/has made for goods and/or services provided by Industrylink Training such as legal name, business trading name, contact names, addresses, telephone numbers, email addresses, ABNs and banking details.
- Information contained in or relating to any communications that are sent to us.

STORAGE OF PERSONAL INFORMATION

Industrylink Training records all student and employer information, as well as copies of communications and interactions in our computerised database, "VETtrak". This is a secure, password protected database. Only selected and trained Industrylink staff have access to view and edit this database. We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of any personal information.

Any paper copies of personal information gathered from a client or an employer, are retained in named files which are stored in the administration office, in securely locked filing cabinets.

USING / DISCLOSING PERSONAL INFORMATION

Personal information submitted to us will be used for the purposes specified at the time of the collection, and for no other purpose. Industrylink will only collect and hold personal information if it is necessary for one or more of its functions or activities. The purpose of collection will be communicated to the individual at the time of collection.

We may disclose personal information to Industrylink employees, insurers, professional advisers, agents, suppliers or subcontractors insofar as reasonably necessary for the purposes of them completing their work duties/responsibilities.

We may disclose personal information:

- to the extent that we are required to do so by law;
- in connection with any ongoing or prospective legal proceedings;
- in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);
- to lessen or prevent a serious threat to an individual's life, health, safety or welfare or a serious threat to public health or safety;
- to the purchaser (or prospective purchaser) of any business or asset that we are (or are contemplating) selling; and]
- to any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information where, in our reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.]

Industrylink Training will not send personal information about an individual outside Australia without:

- Obtaining the written consent of the individual; or
- Otherwise complying with the National Privacy Principles.

Except as provided in this policy, we will not provide your personal information to third parties.

ACCESS TO PERSONAL INFORMATION / FREEDOM OF INFORMATION

On request, Industrylink Training will provide access to an individual, to personal information held about them, and must, if the individual demonstrates that the personal information is incorrect, incomplete, out of date or misleading, request to amend that personal information.

In some circumstances, Industrylink Training may require individuals seeking to access or correct their personal information, to make a written request under the *Freedom of Information Act 1991*, in which case, the decision on the person's right to access or correct the information will be made in accordance with that Act. Freedom of information requests should be made in writing and directed to the C.E.O. for consideration. (for example, a staff member may request access to their personnel file which would be granted without question, however some documents, such as referee checks might not be disclosed, at the discretion of the C.E.O.).

DISPOSAL OF PERSONAL INFORMATION

Industrylink will destroy or permanently de-identify personal information that it no longer needs.

We will ensure that records are disposed of securely and in accordance with any requirements for the retention and disposal of personal information.