Privacy

POLICY

Purpose

The purpose of this policy is to demonstrate that as required by the Australian Privacy Principles, Institute of Research and Learning (IRL) has a privacy policy which outlines how it will deal with and store personal information, as well as manage inquiries and complaints.

Principles

The principles which underpin this policy include:

- IRL respects the privacy of students and is committed to protecting personal information
- By providing personal information to IRL, students consent to its collection, use, storage and disclosure in accordance with this Privacy Policy. IRL is committed to providing flexible learning and assessment options, allowing students alternatives which recognise the diversity of their individual needs and circumstances aiding them in their learning goals
- 'Personal information' has the meaning provided in section 12 of the Information Privacy Act 2009 (Qld) and includes any information that allows a person to be identified including:
    - Name, address, email address, age, gender, USI, contact information occupation, citizenship status, education history
    - tracking information for Google Analytics; and
    - information collected for the IRL Student Management System (SMS)
- This policy applies to all IRL employees, contractors, students, and stakeholders.

Australian Privacy Principles (APP)

The following sections of this policy outline how IRL as a registered training organisation (RTO) ensures its operations are compliant with the Privacy Act 1988 (Cth) and APP requirements.

Australian Privacy Principle 1: Open and transparent management of personal information

The objective of this principle is to ensure that IRL manages personal information in an open and transparent way. This enhances the accountability of IRL for personal information handling practices and can build community trust and confidence in these practices.

IRL retains a record of personal information about all individuals with whom it undertakes any form of business activity.

As a government registered training organisation (RTO), regulated by the Australian Skills Quality Authority (ASQA) IRL is required to collect, hold, use and disclose a wide range of personal and sensitive information on participants in nationally recognised training programs.

This information requirement is outlined in the National Vocational Education and Training Regulator Act 2011 and associated legislative instruments. In particular, the legislative instruments:

- Student Identifiers Act 2014 (Cth)
- Standards for Registered Training Organisations (RTOs) 2015; and
- Data Provision Requirements 2012 (Cth).

IRL is also bound by state government legislation requiring similar information collection, use and disclosure relevant to state jurisdictions of IRL operations.

Aligned with these legislative requirements, IRL delivers services through a range of government funding contract agreement arrangements, which also include various information collection and disclosure requirements.

Individuals are advised that due to these legal requirements, IRL discloses information held on individuals for valid purposes to a range of entities including but not limited to:

- Governments (Commonwealth, State or Local)
- Australian Apprenticeships Support Networks (AASNs)
- Employers (and their representatives), Job Network Providers, schools, guardians; and
- Service providers such as credit agencies and background check providers.

Kinds of personal information held

The following types of personal information are generally collected, depending on the need for service delivery:

- Personal and contact details
- Employment details
- Educational background and academic history
- LLN proficiency
- Demographic information
- Course progress and achievement information; and
- Financial billing information.

The following types of sensitive information may also be collected and held:

- Identity details
- Employee details & HR information
- Complaint or issue information
- Disability status & other individual needs
- Information required for the issuance of a Unique Student Identifier (USI) (Refer to **Attachment 1** for more information regarding USI)
- Indigenous status.

How personal information is collected

IRL's approach to collecting personal information is to collect any required information directly from the individuals concerned. This may include the use of forms (such as registration forms, enrolment forms or service delivery records) and the use of web-based systems (such as online enquiry forms, web portals or internal operating systems).

How personal information is held

IRL's approach to holding personal information always includes robust storage and security measures. Information on collection is:

- As soon as practical converted to electronic means
- Stored in secure, password protected systems, such as financial system, SMS; and
- Monitored for appropriate authorised use at all times.

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role.

IRL has robust access protection with passwords and private keys for authentication. On top of this, the infrastructure sits behind firewalls and only whitelisted IP addresses are allowed to connect. Virus protection, backup procedures and ongoing access monitoring procedures are in place.

Destruction of paper-based records occurs as soon as practicable in every matter, through the use of secure shredding and destruction services.

Retention and destruction of information

The process by which IRL collects, manages, maintains and disposes of student, personnel, finance and other records is outlined in the Student Records and Data Management Policy. Specifically, for RTO related records, in the event of IRL ceasing to operate, the required personal information on record for individuals undertaking nationally recognised training would be transferred to the Australian Skills Quality Authority (ASQA), as required by law.

Accessing and seeking correction of personal information

IRL confirms all individuals have a right to request access to their personal information held and to request its correction at any time. In order to request access to personal records, individuals are in the first instance to contact their trainer.

A number of third parties, other than the individual, may request access to an individual's personal information. Such third parties may include employers, parents or guardians, schools, Australian Apprenticeships Support Networks, Governments (Commonwealth, State or Local) and various other stakeholders. In all cases where access is requested, IRL will ensure:

- Parties requesting access to personal information are robustly identified and vetted
- Where legally possible, the individual to whom the information relates will be contacted to confirm consent (if consent not previously provided for the matter) and
- Only appropriately authorised parties, for valid purposes, will be provided access to the information.

Complaints about breach of the APPs

If an individual feels IRL may have breached one of the APPs, they should follow the complaints procedure which forms part of this policy.

Australian Privacy Principle 2: Anonymity and Pseudonymity

This principle provides that individuals must have an option of not identifying themselves or using a pseudonym when dealing with a registered training organisation (RTO) in relation to a particular matter. The principle does not apply in relation to the following:

Requiring Identification – Required of authorised by law

RTOs in service delivery to clients for nationally recognised course programs are required and authorised by Australian law to deal with individuals who have identified themselves. That is, it is a condition of registration for all RTOs under the National Vocational Education and Training Regulator Act 2011 that RTOs collect and report on the Australian Vocational Education and Training Management of Information Statistical Standard (AVETMISS) data for all participants enrolled in nationally recognised training programs.

Requiring Information – Impracticability

This principle provides that an individual may not have the option of dealing anonymously or by pseudonym with an RTO if it is impractical for the RTO to deal with individuals who have not identified themselves.

The following are examples of where it may be impractical to deal with an individual who is not identified:

- Dispute resolution – it may be impractical to investigate and resolve an individual's particular complaint about how their case was handled unless the complainant provides their name or similar information
- Eligibility for government subsidies or support – in responding to an individual's course inquiries and government subsidy support that may be available, the RTO may not be able to provide that information without knowing the requester's identity and individual characteristics.

IRL acknowledges that anonymity and pseudonymity are important privacy concepts. They enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others.

Whenever practical IRL provides individuals with the option of not identifying themselves, or of using a pseudonym.

a) Anonymity

Anonymity requires that an individual may deal with IRL without providing any personal information or identifiers where possible. In such cases IRL should not be able to identify the individual at the time of the dealing or subsequently. Examples of anonymous dealings include an unidentified individual telephoning IRL to inquire generally about its courses or services.

b) **Pseudonymity**

Pseudonymity requires that an individual may deal with IRL by using a name, term or descriptor that is different to the person's actual name.

Examples include an email address that does not contain the individual's actual name, or generic user names in situations where individuals may access a public component of our website or enquiry forms.

The use of a pseudonym does not necessarily mean that an individual cannot be identified. The individual may choose to divulge their identity, or to volunteer personal information necessary to implement a particular transaction where required practically for service delivery or by law.

Personal information should only be linked to a pseudonym if it is required or authorised by law, it is impractical for the RTO to act differently, or the individual has consented to providing or linking the additional information. IRL only stores and links pseudonyms to individual personal information in cases where this is required for services delivery (such as system login information) or once the individual's consent has been received.

IRL advises individuals of their opportunity to deal anonymously or by pseudonym with us where these options are possible, for example, through surveys or feedback.

Australian Privacy Principle 3: Collection of solicited personal information

Under this principle IRL solicits personal information if it explicitly requests another organisation to provide personal information or takes active steps to collect personal information. Examples of solicited information includes:

- Information provided by an individual or another party in response to requests. This may include information from an individual's parents, employers, schools, Australian Apprentices Support Network, or from government websites and registers.
- A completed form or application submitted by an individual
- A complaint letter sent in response to a general invitation on the RTO's website to individuals to complain to the RTO
- An employment application sent in response to a job advertisement published by the RTO
- A form completed to enter a competition conducted by the RTO
- An entry in the RTO's office visitors' book and
- A record of a credit card payment. Note no credit card details are retained by IRL.

This principle deals with two (2) aspects of collecting solicited personal information:

- When an RTO can collect personal information and
- How an RTO must collect personal information.

In response to the requirements of this principle, IRL:

- Only collects personal information that is reasonably necessary for one or more of its functions or activities
- Only collects sensitive information in cases where the individual consents to the sensitive information being collected, unless an exception applies
- Only collects information by lawful (eg covid 19 management plan) and fair means
- Only collects solicited information directly from the individual concerned unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

Australian Privacy Principle 4: Dealing with unsolicited personal information

This principle outlines the steps IRL takes if it receives unsolicited personal information. Unsolicited personal information is information received by IRL that has not been requested by IRL.

IRL may from time to time receive unsolicited personal information. Where this occurs IRL promptly reviews the information to decide whether we could have collected the information for the purpose of

our business activities. Where this is the case, IRL may hold, use and disclose the information appropriately as per the practices outlined in this policy.

Where IRL could not have collected this information (by law or for a valid business purpose) IRL will immediately destroy or de-identify the information (unless it would be unlawful to do so).

Australian Privacy Principle 5: Notification of the collection of personal information

Whenever IRL collects personal information about an individual, IRL takes reasonable steps to notify the individual of the details of the information collection or otherwise ensures the individual is aware of those matters. This notification occurs at or before the time of collection, or as soon as practicable afterwards.

IRL notifications to individuals on data collection include:

- IRL's identity and contact details, including the position title, telephone number and email address of a contact who handles enquiries and requests relating to privacy matters
- The facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a third party, including the name of that party
- If the collection is required or authorised by law, including the name of the Australian law or other legal agreement requiring the collection
- The purpose of collection, including any primary and secondary purposes
- The consequences for the individual if all or some personal information is not collected
- Other organisations or persons to which the information is usually disclosed, including naming those parties
- Whether we are likely to disclose the personal information to overseas recipients, and if so, the names of the recipients and the countries in which such recipients are located
- Reference to this policy in the Student Handbook which explains how it may be accessed; and
- Advice that this policy contains information about how the individual may access and seek correction of the personal information held by IRL and how to complain about a breach of the APPs and how IRL will deal with such a complaint.

Where possible, IRL will ensure the individual confirms their understanding of these details, such as through signed declarations, website form acceptance of details or in person through questioning.

Collection from Third Parties

Where IRL collects personal information from another organisation, IRL will:

- Confirm whether the other organisation has provided the relevant notice above to the student; or
- Whether the individual was otherwise aware of these details at the time of collection; and
- If this has not occurred, we will undertake this notice to ensure the individual is fully informed of the information collection.

Australian Privacy Principle 6: Use or disclosure of personal information

IRL only uses or discloses personal information it holds about an individual for the primary purposes for which the information was collected, or secondary purposes in cases where:

- An individual consented to a secondary use or disclosure
- An individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection; or
- Using or disclosing the information is required or authorised by law.

Requirement to make a written note of use or disclosure for this secondary purpose

If IRL uses or discloses personal information in accordance with an 'enforcement related activity' (as defined by the APPs, Office of the Australian Information Commissioner), IRL will make a written note of the use or disclosure, including the following details:

- The date of the use or disclosure
- Details of the personal information that was used or disclosed
- The enforcement body conducting the enforcement related activity
- If the organisation used the information, how the information was used by the organisation
- The basis for our reasonable belief that we were required to disclose the information.

Australian Privacy Principle 7: Direct marketing

IRL does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing. If at any time IRL would want to use or disclose personal information for the purposes of marketing, it would not do so unless:

- The personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing; or
- The personal information has been collected from a third party, or from the individual directly, but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing; and
- We provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

On all direct marketing communications, IRL will provide a prominent statement that the individual may request to opt out of future communications, and how to do so.

An individual may also request at any stage not to use or disclose their personal information for the purpose of direct marketing, or to facilitate direct marketing by other organisations.

IRL will promptly comply with any request by an individual.

Australian Privacy Principle 8: Cross-border disclosure of personal information

IRL does not send personal information overseas.

Australian Privacy Principle 9: Adoption, use or disclosure of government related identifiers

IRL does not adopt, use or disclose a government related identifier related to an individual except:

- In situations required by Australian law or other legal requirements
- Where reasonably necessary to verify the identity of the individual

- Where reasonably necessary to fulfil obligations to an agency or a State or Territory authority; or
- As prescribed by regulations.

Australian Privacy Principle 10: Quality of personal information

IRL takes reasonable steps to ensure that the personal information it collects is:

- Accurate
- Up-to-date and
- Complete.

IRL also takes reasonable steps to ensure that the personal information we use or disclose is, also relevant for the purpose or disclosure. This is particularly important:

- When information is initially collected and
- When personal information is used or disclosed.

Quality measures in place supporting these requirements include:

- Internal practices, procedures and systems to audit, monitor, identify and correct poor quality personal information (including training staff in these practices, procedures and systems)
- Protocols that ensure personal information is collected and recorded in a consistent format, from a primary information source when possible
- Ensuring updated or new personal information is promptly added to relevant existing records
- Providing individuals with a simple means to review and update their information on an on-going basis through our online portal
- Reminding individuals to update their personal information at critical service delivery points (such as completion) when we engage with the individual
- Contacting individuals to verify the quality of personal information where appropriate when it is about to be used or disclosed, particularly if there has been a lengthy period since collection; and
- Checking that a third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems.

Australian Privacy Principle 11: Security of personal information

IRL takes active measures to consider whether we can retain personal information we hold and to ensure the security of personal information we hold. This includes reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

IRL will destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

Access to IRL offices and work areas is limited to IRL personnel only - visitors to IRL premises must be authorised by relevant personnel and are always accompanied. With regard to any information in a paper-based form, IRL maintains storage of records in an appropriately secure place to which only authorised individuals have access.

Staff training and information sessions are conducted with IRL personnel on privacy issues, and how the APPs apply to our practices, procedures and systems. IRL conduct ongoing internal audits (at least annually, and as needed) of the adequacy and currency of security and access practices, procedures and systems implemented.

Australian Privacy Principle 12: Access to personal information

Where IRL holds personal information about an individual, IRL provides that individual access to the information on their request. In processing requests, IRL:

- Ensures through confirmation of identity that the request is made by the individual concerned, or by another person who is authorised to make a request on their behalf
- Responds to a request for access:
    - Within 14 calendar days, when notifying our refusal to give access, including providing reasons for refusal in writing, and the complaint mechanisms available to the individual: or
    - Within 30 calendar days, by giving access to the personal information that is requested in the manner in which it was requested.
- Provides information access free of charge.

Australian Privacy Principle 13: Correction of personal information

IRL takes reasonable steps to correct personal information held, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

a) Individual requests

On (written) request from an individual IRL will:

- Correct personal information held; and
- Notify any third parties of corrections made to personal information if this information was previously provided to these parties.

In cases where IRL refuses to update personal information (including deletion), IRL will:

- Give a written notice to the individual, including the reasons for the refusal and the complaint mechanisms available to the individual
- Upon request by the individual whose correction request has been refused, take reasonable steps to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading
- Respond within 14 calendar days to these requests and
- Complete all actions free of charge.

b) Correcting at IRL's discretion

IRL will take reasonable steps to correct personal information in cases where IRL is satisfied that the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading (that is, the information is faulty).

This awareness may occur through collection of updated information, in notification from third parties or through other means.

National Data Management Policy

Background

The National VET Data Policy outlines arrangements for disclosing, accessing and using the VET data held by the National Centre for Vocational Education Research (NCVER) on behalf of state, territory and Commonwealth governments.

Under this policy the Australian Government, Department of Education Skills and Employment (DESE brings together requirements for collecting nationally consistent data about VET activity and processes, and for using data in statistical collections and national surveys.

The current National VET Data Policy is available at - https://www.dese.gov.au/national-vet-data/resources/national-vet-data-policy

Comprehensive and timely data on vocational education and training (VET) is important for increasing the efficiency and transparency of Australia's VET sector, to improve understanding of Australia's VET market and management of the national VET system.

Responsibilities of parties

- IRL is required under the National Vocational Education and Training Regulator Act 2011 (Cth) [NVETR Act]) to disclose the personal information it collects about students to the National VET Data Collection kept by NCVER.
- NCVER is responsible for collecting, managing, analysing and communicating research and statistics about the Australian VET sector.
- IRL is authorised under the NVETR Act to disclose the personal information of its students to the relevant state or territory training authority.
- NCVER is authorised to collect, hold, use and disclose student personal information in accordance with legislation including the Privacy Act 1988 (Cth) (Privacy Act) and the NVETR Act.

Student personal information may be used and disclosed by NCVER for purposes that include:

- Populating authenticated VET transcripts
- Administration of VET
- Facilitation of statistics and research relating to education, including surveys and data linkage; and
- Understanding the VET market.

NCVER is authorised to disclose information to the DESE, Commonwealth authorities, State and Territory authorities (other than registered training organisations) that deal with matters relating to VET and VET regulators for the purposes of those bodies, including to enable:

- Administration of VET, including program administration, regulation, monitoring and evaluation
- Facilitation of statistics and research relating to education, including surveys and data linkage
- Understanding how the VET market operates, for policy, workforce planning and consumer information.

The NCVER may also disclose personal information to persons engaged by NCVER to conduct

research on NCVER's behalf.

IRL is required to explain these processes to students and that fact DESE is authorised by law, including the Privacy Act and the NVETR Act, to collect, use and disclose student personal information to fulfil specified functions and activities. IRL achieves this through the inclusion of a Privacy Notice in all enrolment forms.

Refer to Attachment 2 for a copy of the Privacy Notice which is included in all enrolment forms. This notice has been developed from the information which is contained in Schedule 1 (Minimum mandatory content for inclusion in a Privacy Notice) of the National VET Data policy available at https://www.dese.gov.au/national-vet-data/resources/national-vet-data-policy

Framework for Managing Requests and Incidents

Request for records access

Individuals or third parties may at any stage request access to records held by IRL relating to their personal information.

The following procedure is followed on each individual request for access:

a) A request for access is provided by the requester, with suitable information provided to be able to:

- Identify the individual concerned
- Confirm their identity; and
- Identify the specific information that they are requesting access to.

b) This request is to be made in writing, and in the first instance should be made to the individual's trainer.

c) Upon receiving a request for access, IRL will:

- Confirm the identity of the individual or party requesting access
- Confirm that this individual or party is appropriately authorised to receive the information requested
- Search the IRL records to assess whether the requested personal information is contained in those records; and
- Collate any personal information found ready for access to be provided.

d) Once identity and access authorisation is confirmed, and personal information is collated, access is provided to the requester within 30 calendar days of receipt of the original request. IRL will provide access to personal information in the specific manner or format requested by the individual, wherever it is reasonable and practicable to do so, free of charge. Where the requested format is not practical, IRL will consult with the requester to ensure a format is provided that meets the requester's needs.

e) If the identity or authorisation access cannot be confirmed, or there is another valid reason why IRL is unable to provide the personal information, refusal to provide access to records will be provided to the requester, in writing. Notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual. Such notifications are provided to the requester within 30 calendar days of receipt of the original request.

Request for records update

Individuals or third parties may at any stage request their records (held by IRL and relating to their personal information) be updated.

The following procedure is followed on each individual request for records updates:

a) A request for records update is provided by the requester, with suitable information provided to be able to:

- Identify the individual concerned
- Confirm their identity; and
- Identify the specific information that they are requesting be updated on their records.

This request must be in writing.

b) Upon receiving a request to update records IRL then:

- Confirms the identity of the individual or party to whom the record relates
- Searches the records that IRL possesses or controls to assess whether the requested personal information is contained in those records; and
- Assesses the information already on record, and the requested update, to determine whether the requested update should proceed. This may include checking information against other records held by IRL or within government databases in order to complete an assessment of the correct version of information to be used.

c) Once identity and information assessment is confirmed, personal information is:

- Updated, free of charge, within 14 calendar days of receipt of the original request; and
- Notified to any third parties of corrections made to personal information if this information was previously provided to these parties.

d) If the identity of the individual cannot be confirmed, or there is another valid reason why IRL is unable to update the personal information, refusal to update records will be provided to the requester in writing, free of charge, within 14 calendar days. Notification will include the reasons for the refusal and the complaint mechanisms available to the individual.

e) Upon request by the individual whose correction request has been refused, IRL will also take reasonable steps to associate a 'statement' with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.
This statement will be applied, to all personal information relevant across IRL systems within 30 calendar days of receipt of the statement request.

Complaints management

If an individual feels IRL has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. IRL encourages individuals to discuss the situation with their trainer (or other representative) in the first instance, before making a complaint.

Privacy related complaints are managed through the IRL Complaints and Appeals Policy.

If after following that process the individual is still not satisfied, they can escalate their complaint directly to the Office of the Australian Information Commissioner (OAIC) for investigation. Website address www.oaic.gov.au or phone number 1300 363 992.

When investigating a complaint, the OAIC will initially attempt to conciliate the complaint, before considering the exercise of other complaint resolution powers.

A complaint may also be lodged with the Australian Skills Quality Authority (ASQA) complaints handing service for complaints against RTOs at either the website www.asqa.gov.au or phone 1300 701801.

Attachment 1

Unique Student Identifier (USI) Information

All students participating in nationally recognised training from 1 January 2015, are required to have a Unique Student Identifier (USI) and provide it to the RTO upon enrolment. Alternatively, the RTO can apply for a USI on behalf of an individual.

The Student Identifiers Act 2014 authorises the Australian Government's Student Identifiers Registrar to collect information about USI applicants. When an RTO applies for a USI on behalf of a student who has authorised them to do so, the RTO needs to collect personal information about the student which will be passed on to the Student Identifiers Registrar. This will include:

- Name, including first or given name(s), middle name(s) and surname or family name
- Date of birth
- City or town of birth
- Country of birth
- Gender
- Contact details, so the student identifiers registrar can provide individuals with their USI and explain how to activate their USI account.

To create a USI on behalf of a student, an RTO will be required to verify the identity of the individual by receiving a copy of an accepted identification document.

This document will only be used for the purposes of generating the USI and confirming the identity of the individual with the Registrar.

Once the USI has been generated and validated, the identity documents used or collected for this purpose will be securely destroyed.

The information provided by an individual in connection with their application for a USI:

- Is collected by the Registrar as authorised by the Student Identifiers Act 2014.
- Is collected by the Registrar for the purposes of:
  - Applying for, verifying and giving a USI
  - Resolving problems with a USI
  - Creating authenticated vocational education and training (VET) transcripts
- May be disclosed to:
  - Commonwealth and State/Territory government departments and agencies and statutory bodies performing functions relating to VET for:
    - The purposes of administering and auditing VET, VET providers and VET programs
    - Education related policy and research purposes
    - To assist in determining eligibility for training subsidies
  - VET Regulators to enable them to perform their VET regulatory functions
  - VET Admission Bodies for the purposes of administering VET and VET programs
  - Current and former Registered Training Organisations to enable them to deliver VET courses to the individual, meet their reporting obligations under the VET standards and government contracts and assist in determining eligibility for training subsidies

- Schools for the purposes of delivering VET courses to the individual and reporting on these courses.

The National Centre for Vocational Education Research (NCVER) for the purpose of creating authenticated VET transcripts, resolving problems with USIs and for the collection, preparation and auditing of national VET statistics.

- Researchers for education and training related research purposes
- Any other person or agency that may be authorised or required by law to access the information
- Any entity contractually engaged by the Student Identifiers Registrar to assist in the performance of his or her functions in the administration of the USI system

Will not otherwise be disclosed without the student's consent unless authorised or required by or under law.

The consequences to the student of not providing the Registrar with some or all of their personal information are that the Registrar will not be able to issue the student with a USI, and therefore the RTO will be unable to issue a qualification or statement of attainment.

Attachment 2

Privacy Notice

Why we collect your personal information

As a registered training organisation (RTO), IRL collects collect your personal information so we can process and manage your enrolment in a vocational education and training (VET) course with us.

Without this information you would not be able to be enrolled as a student.

How we use your personal information

IRL uses your personal information to enable us to deliver VET courses to you, and otherwise, as needed, to comply with our obligations as an RTO.

How we disclose your personal information

IRL is required by law (under the National Vocational Education and Training Regulator Act 2011 (Cth) (NVETR Act)) to disclose the personal information we collect about you to the National VET Data Collection kept by the National Centre for Vocational Education Research Ltd (NCVER).

The NCVER is responsible for collecting, managing, analysing and communicating research and statistics about the Australian VET sector.

We are also authorised by law (under the NVETR Act) to disclose your personal information to the relevant state or territory training authority.

How the NCVER and other bodies handle your personal information

The NCVER will collect, hold, use and disclose your personal information in accordance with the law, including the Privacy Act 1988 (Cth) (Privacy Act) and the NVETR Act.

Your personal information may be used and disclosed by NCVER for purposes that include populating authenticated VET transcripts; administration of VET; facilitation of statistics and research relating to education, including surveys and data linkage; and understanding the VET market.

The NCVER is authorised to disclose information to the Australian Government Department of Education, Skills and Employment (DESE), Commonwealth authorities, State and Territory authorities (other than registered training organisations) that deal with matters relating to VET and VET regulators for the purposes of those bodies, including to enable:

- Administration of VET, including program administration, regulation, monitoring and evaluation
- Facilitation of statistics and research relating to education, including surveys and data linkage
- Understanding how the VET market operates, for policy, workforce planning and consumer information.

The NCVER may also disclose personal information to persons engaged by NCVER to conduct research on NCVER's behalf. The NCVER does not intend to disclose your personal information to any overseas recipients.

For more information about how the NCVER will handle your personal information please refer

to the NCVER's Privacy Policy at www.ncver.edu.au/privacy.

If you would like to seek access to or correct your information, in the first instance, please contact your RTO using the contact details listed below.

DESE is authorised by law, including the Privacy Act and the NVETR Act, to collect, use and disclose your personal information to fulfil specified functions and activities. For more information about how the DESE will handle your personal information, please refer to the DESE VET Privacy Notice at https://www.dese.gov.au/national-vet-data/vet-privacy-notice.

Surveys

You may receive a student survey which may be run by a government department or an NCVER employee, agent, third-party contractor or another authorised agency.

Please note you may opt out of the survey at the time of being contacted.

Contact information

At any time, you may contact IRL to:

- Request access to your personal information
- Correct your personal information
- Make a complaint about how your personal information has been handled
- Ask a question about this privacy notice.