Privacy Policy

Collecting and handling personal information is a necessary part of conducting our RTO's operations. Essential Skills Training and Recruitment (ESTR) will manage personal information in accordance with all legal and ethical requirements regarding the collection, storage and disclosure of the personal information it holds about individuals.

This policy has been aligned to the Australian Privacy Principles (AAP).

Supporting policies and procedures

The following policies and procedures support this Privacy policy and procedure;

- PP-006 Marketing and Advertising
- PP-018 Student Enrolment and Pre-Training Review
- PP-023 Employment Checks - CRC & WWCC
- PP-028 Records Management
- PP-034 Unique Student Identifier Policy
- PP-035 Traineeships Policy
- PP-036 Students under 18 Policy
- PP-049 Government Subsidy Eligibility Requirements
- PP-054 Complaints and Appeals Policy

Privacy Procedures

Types of information collected and held

- The following types of personal information is collected and held, depending on the need for service delivery;
    - Contact details
    - Identity details and proof of identification
    - Proof of citizenship where relevant
    - Employment details where relevant
    - Proof to support the eligibility for a concession fee where relevant
    - Background information about prior education, schooling, place of birth, disability status, Indigenous status etc. for statistical purposes
    - Unique Student Identifiers i.e. USI, VSN
    - Financial billing information
    - Background checks such as National Criminal Record Checks and/or Working with Children checks
    - Course progress and achievement information
    - Employee details and HR information

How information is collected

- ESTR collects information only by lawful and fair means, and only collects personal information that is reasonably necessary for our business activities. We only collect sensitive information in cases where the individual consents to the sensitive information being collected, except in cases where we are required to collect this information by law, such as outlined in this policy.

- Personal information is generally collected as part of the enrolment application pre-training review process or ESTR employee onboarding process.
- ESTR's usual approach is to collect any required information directly from the individuals concerned however ESTR also receives information from third party sources in undertaking service delivery activities including;
    - Australian Apprenticeship Centres
    - Employers, Job Network Providers, Schools, Guardians
    - Background check providers
    - Governments (Commonwealth, State or Local)

How information is held and security measures for personal information

- ESTR will ensure all reasonable steps to protect information collected and held from misuse, interference and loss, unauthorised access, modification or disclosure.
    - Information on collection is entered and stored electronically in secure, password protected systems, such as our financial system Xero and learning/student management system aXcelerate.
    - Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role.
    - Internal security measures are in place for our physical server system access. Virus protection, backup procedures and ongoing monitoring procedures are in place with our dedicated IT department – Hardy IT. .
    - Paper-based records are kept confidential and stored in appropriately secure places in ESTR offices and work areas.
    - Access to ESTR's offices and work areas is limited to ESTR staff only. Students and visitors are not authorised to access staff areas unless they are accompanied by an ESTR employee at all times.

Purposes for the collection, retention, use and disclosure of information

- Information collected by ESTR is used to;
    - enable efficient student administration,
    - provide information about training opportunities,
    - issue statements of attainment and qualifications to eligible students, and
    - to maintain accurate and detailed records of student course participation, progress and outcomes.
- As a Government Registered Training Organisation, regulated by the Australian Skills Quality Authority (ASQA) and bound by various State Government Acts, ESTR is required to collect, hold, use and disclose a wide range of personal information on participants in nationally recognised training programs in accordance with the following legislation;
    - *National Vocational Education and Training Regulator Act 2011*
    - *Student Identifiers Act 2014;*
    - *Standards for Registered Training Organisations (RTOs) 2015;*
    - *Data Provision Requirements 2012;* and
    - *Apprenticeship and Traineeship Act 2001*

- Also aligned with the above-mentioned legislative requirements, ESTR delivers services through a range of Commonwealth and State Government funding contract arrangements, which also include various information collection and disclosure requirements.
- Students are advised as part of the enrolment application pre-training review process that due to these legal requirements, ESTR discloses information held on individuals for valid purposes to a range of entities including:
    - Commonwealth and State or Territory government departments and authorised agencies, particularly those that support or fund the training
    - Australian Apprenticeships Centres;
    - Employers (and their representatives),
    - Job Network Providers,
    - Schools,
    - Guardians;
    - Service providers such as background check providers
    - Australian Quality Skills Authority (ASQA)
    - National Centre for Vocational Education Research Ltd (NCVER)
    - Organisations conducting student surveys and researchers
- ESTR ensures that the individual confirms their understanding of these details through signed declarations, website form acceptance of details or in person through questioning.

Anonymity and pseudonymity

- In accordance with the Privacy Act, ESTR will provide individuals with the option of not identifying themselves or using a pseudonym, when dealing with us in relation to a particular matter, **whenever practical**. This includes providing options for anonymous dealings in cases of general course enquiries or other situations in which an individuals' information is not required to complete a request. However, there are occasions within our service delivery where an individual may not have the option of dealing anonymously or by pseudonym, as identification is practically required for us to effectively support an individual's request or need.
- It is a *Condition of Registration* for all RTOs under the *National Vocational Education and Training Regulator Act 2011* that we identify individuals and their specific individual needs on commencement of service delivery, and collect and disclose Australian Vocational Education and Training Management of Information Statistical Standard (AVETMISS) data on all individuals enrolled in **nationally recognised training programs**. Other legal requirements, as noted earlier in this policy, also require considerable identification arrangements.

Use or disclosure of personal information

- ESTR takes reasonable steps to ensure that the personal information we use or disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. Quality measures in place supporting these requirements include;
    - 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 their online student portal.

- ESTR only uses or discloses personal information it holds about an individual for the particular 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.
- ESTR does not disclose any information to any overseas recipients.
- ESTR may from time to time receive unsolicited personal information. Where this occurs we promptly review the information to decide whether or not we could have collected the information for the purpose of our business activities. Where this is the case, we may hold, use and disclose the information appropriately as per the practices outlined in this policy. Where we could not have collected this information (by law or for a valid business purpose) we immediately destroy or de-identify the information (unless it would be unlawful to do so).
- ESTR does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, 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
- On each of our direct marketing communications, ESTR provides a prominent statement that the individual may request to opt out of future communications, and how to do so.

Adoption, use or disclosure of government related identifiers

- ESTR 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.
- It is unlawful under the Privacy Act 1988 and the Taxation Administration Act 1953 for ESTR to request, record, maintain a record of, use or disclosure a **student's Tax File Number (TFN).** ESTR will never request a tax file number, however, if a student incidentally provides information that contains a TFN e.g. ATO Notice of Assessment, we will take reasonable steps to securely destroy or permanently de-identify the TFN information. Where possible, the preference is always to destroy TFN information.

Retention and destruction of information

- ESTR maintains a retention and disposal schedule documenting the periods for which personal information records must be kept.in accordance with legislative requirements as outlined in PP-028 Records Management.
- ESTR 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.
- The ESTR Leadership Team will arrange for paper-based records to be securely shredded once the retention of records timeframe expires.
- Specifically, for our RTO records, in the event of our organisation ceasing to operate the required personal information on record for individuals undertaking nationally recognised training with us would be transferred to the Australian Skills Quality Authority (ASQA), as required by law.

Accessing and seeking correction of personal information

- All individuals have a right to request access to their personal information held and to request its correction at any time. If individuals wish to access any of their personal information that we hold, they must submit a written request to info@essentialskills.com.au and provide two (2) forms of identification before the information will be released. There is no fee to access copies of personal information, however if there is a large volume of information we may charge a reasonable administrative fee for photocopying, which individuals will be notified of beforehand.
- 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 Centres, Governments (Commonwealth, State or Local) and various other stakeholders.
- In all cases where access is requested, ESTR will ensure that:
  - Parties requesting access to personal information are robustly identified,
  - 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.

- ESTR takes reasonable steps to correct personal information we hold in cases where we are 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.

Complaints about a breach of this privacy policy

- If an individual feels that ESTR may have breached this privacy policy they are entitled to make a formal complaint. The process for making a complaint is outlined in PP-054 Complaints and Appeals Policy, which is available on our website https://essentialskills.com.au/individuals/

Data breach response procedures

- When responding to a breach or suspected breach the ESTR Leadership Team will, on a case-by-case basis, undertake an assessment of the risks involved, and use that risk assessment as the basis for deciding what actions to take in the circumstances. The following steps will be followed;

Step 1: Contain	Contain the breach and make a preliminary assessment: • Take immediate steps to contain breach. • Designate person/team to coordinate response.
Step 2: Evaluate	Evaluate the risks for individuals associated with the breach: • Consider what personal information is involved. • Determine whether the context of the information is important. • Establish the cause and extent of the breach. • Identify what is the risk of harm.

Step 3: Notify	Consider breach notification:
	• Risk analysis on a case-by-case basis.
	• Not all breaches necessarily warrant notification.
	• Should notifications occur?
	Where there is a real risk of serious harm, notification may enable individuals to take steps to avoid or mitigate harm. Consider:
	  • Legal/contractual obligations to notify.
	  • Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities.
	• Process of notification:
	  • When? As soon as possible.
	  • How? Direct contact if possible (mail/phone).
	  • Who? The affected individual.
	  • What? Description of the breach, type of personal information involved, steps to help mitigate, contact details for information and assistance, other actions underway
	• Should others be notified:
	  • Australian Skills Quality Authority?
	  • Office of the Australian Information Commissioner?
	  • Police/Law Enforcement?
	  • Other organisations affected by the breach or contractually required to notify?

Step 4: Prevent reoccurrence	Review the incident and take action to prevent future breaches: • Fully investigate the cause of the breach. • Consider developing a prevention plan. • Option of audit to ensure plan implemented. • Update security/ response plan. • Make appropriate changes to policies and procedures. • Revise staff training practices.

Endorsed: 25/08/2020 **Version:** 2.0

CEO Signature: Leisa Harrison **Review Date:** August 2020

Compliance References

- Privacy Act 1988;
- Australian Privacy Principles (APPs) as outlined in the Privacy Amendment (Enhancing Privacy Protection) Act 2012;
- National Vocational Education and Training Regulator Act 2011;
- Student Identifiers Act 2014;
- Standards for Registered Training Organisations (RTOs) 2015;
- Data Provision Requirements 2012;
- The Notifiable Data Breaches (NDB) scheme;
- Apprenticeship and Traineeship Act 2001;
- Taxation Administration Act 1953;
- Spam Act 2003.
- Freedom of Information Act 1982