Privacy Policy

Introduction

Skills Network takes the privacy of our students very seriously and we will comply with all legislative requirements. These include the Privacy Act and Australian Privacy Principles January 2014

https://www.oaic.gov.au/privacy/australian-privacy-principles/read-the-australian-privacy-principles

In some cases as required by law and as required by the NVR Standards we will need to make your information available to others. In all other cases we ensure that we will seek the written permission of the student.

Privacy Principles

The Privacy Principles are listed below, with the open and transparent management of personal information defined:

1. **Australian Privacy Principle 1** - open and transparent management of personal information
    a. **Collection** - We will collect only the information necessary for one or more of our functions. The individual will be told the purposes for which the information is collected.
    b. **Use and disclosure** - Personal information will not be used or disclosed for a secondary purpose unless the individual has consented or a prescribed exception applies
    c. **Data quality** - We will take all reasonable steps to make sure that the personal information we collect, use, or disclose is accurate, complete and up to date
    d. **Data Security** - We will take all reasonable steps to protect the personal information we hold from misuse and loss and from unauthorised access, modification, or disclosure
    e. **Openness** - We will document how we manage personal information and when asked by an individual, will explain the information we hold, for what purpose and how we collect, hold, use and disclose the information
    f. **Access and correction** - The individual will be given access to the information held except to the extent that prescribed exceptions apply. We will correct and update information errors described by the individual
    g. **Unique Identifiers** - Commonwealth Government identifiers (Medicare number or tax file number) will only be used for the purposes for which they were issued. We will not assign unique identifiers except where it is necessary to carry out our functions efficiently
    h. **Anonymity** - Wherever possible, we will provide the opportunity for the individual to interact with external agencies without identifying themselves
    i. **Trans-border Data Flows** - The individual's privacy protections apply to the transfer of personal information out of Australia
    j. **Sensitive Information** - We will seek the consent of the individual when collecting sensitive information about the individual such as health information, or information about the individual's racial or ethnic background, or criminal record
2. **Australian Privacy Principle 2** - anonymity and pseudonymity
3. **Australian Privacy Principle 3** - collection of solicited personal information
4. **Australian Privacy Principle 4** - dealing with unsolicited personal information
5. **Australian Privacy Principle 5** - notification of the collection of personal information
6. **Australian Privacy Principle 6** - use or disclosure of personal information
7. **Australian Privacy Principle 7** - direct marketing
8. **Australian Privacy Principle 8** - cross-border disclosure of personal information
9. **Australian Privacy Principle 9** - adoption, use or disclosure of government related identifiers
10. **Australian Privacy Principle 10** - quality of personal information
11. **Australian Privacy Principle 11** - security of personal information
12. **Australian Privacy Principle 12** - access to personal information
13. **Australian Privacy Principle 13** - correction of personal information

Privacy Policy

Collection of information

Skills Network requests information from students as part of the pre-enrolment, enrolment and any re enrolment processes. Skills Network staff will not collect personal information at any time by unlawful or unfair means.

Skills Network will always take reasonable measures to ensure that the individual is made aware of why personal information is being collected and what it could be used for.

Skills Network will only collect students' personal information for the following purposes:

- For the essential communication for the student's safety and comfort during their studies
- When it is necessary for Skills Network to make contact with a student's nominated family member in the case of emergency or accident.
- Selected student details are also collected and used for:
- Processing enrolments
- Enquiries regarding courses available and sending out course information
- Communicating accurately with students
- Assisting students with courses they may be interested in
- Assisting students with RPL applications
- Student account details
- Assessing an individual student's entitlements for government funded areas.

Skills Network will ensure that when personal information is collected it will not intrude to an unreasonable extent into the personal affairs of the prospective student / employee and that the information is up to date and complete.

Disclosure of information

Privacy and confidentiality are paramount within Skills Network and policies and procedures will be observed by all staff. Personal information will not be released without the consent of the student. Skills Network does not release or sell students' personal details to any external companies for the purposes of marketing.

Skills Network may from time to time be required to provide personal information to external organisations including the Australian Government and other designated authorities in order to provide specific services as required by law.

These may include but are not limited to:

- Australian Standards Quality Authority (ASQA)
- State Funding Bodies
- National Centre for Vocational Education Research (NCVER)

The Privacy Notice and Student Declaration is a statement acknowledged by a student during their enrolment to indicate awareness that personal information collected from the student may be used together with training activity information. The privacy statement lists the ways information about the student is held, used, disclosed and managed. For more information in relation to this policy please refer to: https://www.education.gov.au/privacy-notice-and-student-declaration

If there is a serious health-related issue and some information may be provided to Skills Network during a consultation with a practitioner, then this information may be accessed by Skills Network staff for the purposes of providing further helpful services to the student. No other parties will gain access to the information at any time, other than those listed above without the written consent of the individual student concerned.

NCVER

VET Data Use Statement

Under the *National Vocational Education and Training Regulator (Data Provision Requirements) Instrument 2020* and National VET Data Policy (which includes the National VET Provider Collection Data Requirements Policy at Part B), Registered Training Organisations are required to collect and submit data compliant with AVETMISS for the National VET Provider Collection for all Nationally Recognised Training. This data is held by the National Centre for Vocational Education Research Ltd (NCVER), and may be used and disclosed for purposes that include:

- populating authenticated VET transcripts
- administering VET, including program administration, regulation, monitoring and evaluation
- facilitating statistics and research relating to education, including surveys and data linkage
- understanding how the VET market operates, for policy, workforce planning and consumer information.

NCVER is authorised by the *National Vocational Education and Training Regulator Act 2011* (NVETR Act) to disclose to the following bodies, personal information collected in accordance with the Data Provision Requirements or any equivalent requirements in a non-referring State (Victoria or Western Australia), for the purposes of that body:

- a VET regulator (the Australian Skills, Quality Authority, the Victorian Registration and Qualifications Authority or the Training Accreditation Council Western Australia)
- the Australian Government Department of Employment and Workplace Relations
- another Commonwealth authority
- a state or territory authority (other than a registered training organisation) that deals with or has responsibility for matters relating to VET.

NCVER may also disclose personal information to persons engaged by NCVER to conduct research on NCVER's behalf.

Breaches in Privacy and Confidentiality

Should Skills Network become aware of any breach in these Policies and Procedures, Skills Network must promptly consider whether such an incident breaches our obligations under the Privacy Act and the Australian Privacy Principles, and whether Skills Network is required to notify the Office of the Australian Information Commissioner (OAIC) and any parties who are at risk because of the breach.

Procedures

Ensuring the data quality

Consistent with the Australian Privacy Principles, Skills Network is committed to ensuring that personal information collected by Skills Network remains accurate, complete and up to date.

Skills Network relies on its students to advise Skills Network of changes that may occur in personal information in order to keep all records up to date and of good quality.

Skills Network will ensure that the students' records are kept updated by making the changes in the student files, in the student management system and in the student soft copy register as soon as they are provided by the student.

Skills Network will destroy records relating to personal information when such information is no longer necessary to be retained within Skills Network's records. Personal information will be destroyed by shredding or other secure process.

Access to data and making corrections

All students and clients have the right to inspect their own personal information and files held by Skills Network.

Prospective students are informed that upon giving Skills Network their personal contact details, Skills Network will use these details to process their enquiry and send them course information.

Upon reasonable request and 5 working days' notice, Skills Network administrative staff will provide a student with access to their personal records and if required, reissue statements of attainment or qualifications achieved. Skills Network will not allow this to take place without an appointment being made.

Student's personal records cannot be released to parents, partners or any external party without the written consent of the student.

When a record is found to be incorrect, this will be corrected; when a student requests that a record be corrected because it is not accurate or correct, the details of the request for amendment with the evidence supplied for change will be noted on the records.

Breaches of the Privacy Act

Skills Network will take appropriate, prompt action if it has reasonable grounds to believe that a Breach may have, or is suspected to have occurred, by reporting all notifiable data breach matters to the Office of the Australian Information Commissioner (OAIC), individuals to whom the information relates, or taking remedial internal action, depending on the type of data breach. Not all data breaches will require OAIC notification Our Privacy Officer is responsible for managing data breach incidents.

A “Notifiable Data Breach” is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by us is lost or subjected to unauthorised access or disclosure.

Data Breaches (suspected and actual) must be reported to our Privacy Officer who will:

- in conjunction with the reporter of the data breach and any other relevant staff or Licensed Partner, ensure immediate action is taken to mitigate or remove the suspected source of the Data Breach where possible
- have regard to the nature of the breach and the sensitivity of the personal information determine if any remedial action is appropriate to avoid serious harm occurring
- if remedial action is not appropriate, determine if the incident should be escalated to the Data Breach Response Team.

If remedial action is unsuccessful and the data breach will likely result in serious harm to any of the individuals to whom the information relates, the CEO and Compliance Manager will manage the incident.