Department Retail Institute – RTO (ID4049)		
Document ID RI_RTO_015	**Title** Student Information Handling – Policy and Procedures	**Effective** July 2022
Version ID No.1	**Superseding Version** Nil	**Effective** July 2022
Associated Instrument/s	Online enrolment and various paper-based enrolment forms and applicable declarations.	
Approved by Aaron Hines Director, ARA Retail Institute	**Next Review** July 2023	Once printed, this document is not controlled.

1. Policy objective

1.1. The objective of this Policy and procedure is to ensure that the ARA, via its training division, the ARARI, comply with the responsibilities set by law as a nationally recognised RTO.

1.2. This Policy ensures compliance with the Privacy Act 1988 (Cth) and Australian Privacy Principles (APP).

1.3. The ARARI, through the application of this Policy, will:

1.3.1. Implement an APP Policy (3 & 5) when collecting data for the National VET Provider Collection

1.3.2. Specify the requirements of government-related identifiers

1.3.3. Explain how information and data related to students are used.

2. Definitions

2.1. For the purpose of this Policy, and associated Procedures, the following definitions apply:

2.1.1. A training course - is defined as a pathway to achieving a nationally recognised qualification or skill set from an NRT package as listed on the ARA's Scope of Registration.

- For more information, go to the website: training.gov.au - About

2.1.2. ARA – Australian Retailers Association

2.1.3. ARARI – ARA Retail Institute, the entity responsible for administering the ARA's RTO.

2.1.4. USI – the Unique Student Identifier scheme administrated by the USI Registrar.

2.1.5. PII – Personally, Identifiable Information

2.1.6. NCVER - National Centre for Vocational Education Research

2.1.7. Notifiable breach – A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency,

you must notify affected individuals and us when a data breach involving personal information is likely to result in serious harm. Reference: www.oaic.gov.au/privacy/notifiable-data-breaches

- Government-related related identifiers – Refer to Chapter 9: APP9 – Adoption, use of government-related identifiers of the APP Guidelines. A government-related identifier is an identifier that has been assigned by an agency, a State or Territory authority, an agent of an agency or authority, or a contracted service provider for a Commonwealth or State contract.

Scope

3.1. This Policy applies to all individuals who must ensure the ARARI complies with the Standards for RTOs and other laws and conforms to its conditional arrangements with other interested parties critical to the operations of the ARARI. Including:

- any student enrolled and participating in a nationally recognised training program within ARA's Scope of Registration,
- all ARARI staff and or other persons ("other" individuals engaged by the ARA) who facilitate student enrolment,
- all ARA Partners ("Partners" Third Party Arrangements/Agents and staff), and
- all ARARI Directors and the ARA CEO.

3. Related Documents

USI Requirements – Policy and procedures

Record Management – Policy and procedures

Participants Handbook

ARA RTO Privacy Statement and VET Data Statement and Declaration

4. Other interested parties to this Policy

Australian Government – Office of the Australian Information Commissioner

5. Policy

5.1. The ARARI employs the following principles when handling the personal information of students or staff to other parties.

5.1.1. The ARARI will ensure that students are aware of the mandatory use or release of information and data to government agencies.

- Please refer to the ARARI policy and procedures pages on the ARA website relating to the Unique Student Identifier Scheme.
- Please refer to the ARARI compliance pages on the other ARA website relating to the ARA RTO Privacy Statement and VET Data Statement and Declaration.

5.1.2. The ARARI will ensure that releasing the personal information of students and staff to other parties will not be done without the written consent of individuals and the verification of both parties before releasing information.

5.1.3. The ARARI is committed to ensuring that staff and individuals engaged by the ARARI to deliver services are appropriately trained to ensure they are aware of the privacy requirements and how to manage personal information correctly.

5.1.4. The ARARI will ensure that when student records are updated, it is done with proper verification.

5.1.5. The ARARI will ensure there are processes in place to reduce the risk of breaches of privacy requirements by ensuring that staff and individuals engaged on behalf of the RTO to deliver services are aware of their obligations and how to adhere to requirements.

APP Policy

5.2. The ARARI will ensure through the adoption of information security processes and will ANNUALLY review information security practices related to APP 3 and 5. This approach to self-assurance and governance meets the e requirements that from 1 January 2018, all RTOs must comply with APP in the Privacy Act 1988 (Cth) when collecting data for the National Vet Provider Collection, NCVER.

5.2.1. Reasonable steps are taken to implement new practices and procedures, and systems that will ensure compliance with APP 1 – Open and transparent management of personal information

5.2.2. Ensure that sensitive and personal information that the RTOs are required to collect is collected following higher protection in APP 2 – Anonymity and pseudonymity; APP 3 – Collection of personal and sensitive information; APP – 5 Notification of collection.

5.2.3. The ARARI will ensure that it maintains a Privacy Statement, which is updated on the ARARI compliance pages of the ARA Website and other related documents used for the enrolment and admission of students into training courses.

5.2.4. The ARA will ensure that its VET Data Statement and Declaration are maintained YEARLY and updated on the ARA website.

5.3. The ARARI will also take key actions related to all other relevant APP identified as critical to information security and subsequent record-keeping behaviours related to safeguarding PII, including collection, storage, transmission, sharing and disposal.

5.3.1. See appendix one.

5.4. The ARARI provides training to staff and all individuals engaged by the RTO to provide services that are aware of the ARA's information security policies related to data security.

5.5. The ARARI, by utilising the ARA technologies and facilities, ensure processes are in place to meet record-keeping requirements related to government Contracts or Deeds to supply services.

6. Procedures

Collection of personal information

6.1. Information should only be collected where it is necessary to conduct a particular function or administrative activity within the ARARI. For example, administration of student enrolments onto relevant government-related secure online systems or reporting of data on their progress to the National VET Data Collector, NCVER,

6.2. Where the information is not required for any specific purpose, it should not be collected.

6.3. If personal information is likely to be used for other purposes, this should be during the pre-enrolment and admission of a prospective student.

Access to and use of personal information stored in records

6.4. There are several essential principles that staff or individuals engaged by the ARARU to deliver services should consider when dealing with personal information held by the ARARI:

6.4.1. Personal information should be accessed and used only for ARARI purposes, therefore:

- Access to either paper-based digitalised or computerised records should only be granted where there is a demonstrated need for this because of functions or responsibilities within the ARARI Department.
- Even where access is granted, it would be inappropriate, for instance, if an address, home telephone number or other information was accessed and used for private reasons

Personal information should be secured.

6.5. Paper-based records should not be left where public members or others to whom the information they contain is not generally made available may access them. Documents containing personal information should be filed securely behind locked facilities.

6.6. Appropriate arrangements should be implemented within the ARARI Department to ensure that access to computerised and digitalised records is granted only to staff or individuals by the ARARI to deliver services requiring such access during their daily operational duties.

6.7. ARARI Staff or anyone engaged by the ARARI to deliver services should never disclose any passwords to any systems where they are granted privileged access for required administrative duties, data entry and reporting of student information.

6.8. Personal information may only be reported to government bodies, agencies or authorities that require reporting of Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) information data or other records relating to a subsided funding agreement with the ARA. This requirement must be fully disclosed before a student commences a program or study pathway.

6.9. As a general rule, information not expected to be publicly known concerning staff, individuals engaged by the ARARI to deliver services and students should be treated as confidential. It should not be disclosed to anyone but ARARI staff and those involved by the RTO to provide training services who demonstrate the need for this information to carry out their duties. There are several exceptions to this general rule:

6.9.1. <u>Disclosure to the staff member or student to whom the personal information relates:</u>

- Information privacy principles entitle those about whom information is held to access that information. This enables them to ensure that their information is accurate, relevant, up-to-date, complete, and not misleading. Thus, a staff member or a student would be entitled to request access to their file or view information about them in computerised formats. This general entitlement is given effect by the state and territorial Right to Information laws and is subject to its detailed provisions.
- In most cases where access is requested, it will be possible to obtain access without requiring a formal application under these laws. For further advice on handling requests, refer to the ARARI Student Services Department - Email: training@retail.org.au.
- Sometimes, persons supply original documents to the ARARI, such as birth certificates or certified academic records of study undertaken elsewhere. Where it is practicable, original documents provided by a person must be returned to them and must be returned upon request. If this occurs, ARARI records relevant to the transaction must include a photocopy and an annotation indicating that original documents have been sighted and returned.

6.9.2. Disclosure to third parties only with the consent of the student or staff member concerned:

- Personal information may be disclosed to third parties with the consent of the student, staff, or individual engaged by the ARARI to deliver services.
- Such consent cannot be assumed and should be given in writing.
- It cannot be, for instance, considered not to be deemed as implied consent to routinely supply student details to professional associations, potential employers, or government agencies without their prior consent.
- The fact that the enquirer may hold an official position, for example, as an officer of a government department, or in some other way may claim a certain or even official right to get information, makes no difference to this position. Nor does it matter whether the enquiry is made informally using a formal written document.
- Details of a student's academic record should not be given to third parties. Suppose an enquiry concerning a student's record is made by a person or body having a valid reason for seeking the information, e.g., another RTO or prospective employer forwarding details of the record furnished to the enquirer by the student. In that case, the enquiry should be referred to the ARARI Student Services Department - Email: training@retail.org.au, who will, if appropriate, verify the record so furnished.

6.9.3. Disclosure of matters of public record:

- There is a limited amount of personal information held by the ARARI, which amounts to a matter of public record. A notable example is the status of a student's completion of competencies or a training course offered by the ARARI or a reference check. However, unless the ARARI has written consent, it will disclose any sensitive or personal information to any enquirer.
- It should not automatically be assumed that divulging innocuous information, such as information about staff, Trainer/Assessor, or anyone whom the ARARI engages in delivering services, is acceptable.

6.9.4. Disclosure of personal information under statutory or other legal authority:

- In some cases, legislation has conferred upon certain public officers the right to demand and receive information, even though it would otherwise be confidential. A typical example is the Income Tax Assessment Act, under which the Commissioner can authorise officers of that department to require any person to answer any question or to produce any document for inspection. Other Commonwealth Departments may also have powers to obtain access to personal information in specific circumstances.
- In cases where enquiries are received from public officials, the relevant statutory authority to obtain access to such information should be requested.
- Statutory authority should be detailed in writing, as should written verification of appointment as a person entitled to require the information. When this authority is produced, the enquiry should be referred to ARA legal for advice.
- Until such confirmation is obtained, an inspection of ARARI documents is not permitted, no personal information should be released verbally, and copies of documents should not be provided.
- Similarly, where disclosure is sought in the course of legal proceedings, e.g., by service of a subpoena or writ of third-party discovery, this must be referred promptly to ARA legal for action.

6.9.5. Disclosure in instances of wrongdoing associated with ARARI activities."

- Where staff suspect that some record falsification or other wrongdoing has occurred. Report any concerns directly to the Student Services Department, Director of the ARARI or ARA COO.
- At no time should staff disclose such information directly to entities outside the ARA.
- Suppose police officers are involved in investigations of offences associated with ARARI activities or the misuse of ARARI property or systems. In that case, they will make enquiries for personal information about staff or students to assist with their investigations. In exceptional circumstances, the ARARI may consider releasing such information. All such questions must still be referred to ARA legal.

6.9.6. Disclosure for desktop auditing:

- Occasionally, the ARARI must demonstrate evidence of meeting contract arrangements to supply government-subsidised training on behalf of the commonwealth, state, or territories.
- This will result in sensitive and personal information being disclosed. While this is part of the general use of information under the Privacy Statement, the use of this information must only be for the purpose requested by a departmental officer.
- The ARARI should also request a secure file transfer method to transmit all information.

Grievance Procedure

6.10. Students, please discuss Privacy concerns with your Trainer/Assessor, Program Manager or the ARARI Services Department. If Students believe their privacy has been breached. A grievance may be lodged via the online complaints and appeals form. To enable such a complaint to be investigated appropriately, it should identify the person whose privacy appears to have been breached. Anonymous complaints will not be accepted.

6.11. The ARARI complaints and appeals policy and related forms are maintained on the ARARI policies and procedures pages on the ARA Website

6.12. ARARI staff and individuals engaged in delivering services on behalf of the ARA, please discuss Privacy related issues with your immediate report, the ARA COO or CEO.

Appendix 1. Reference:

VETR - Australian Privacy Principles – Implementation Guide for RTOs

The following table outlines some of the key factors to be considered as RTOs plan for their implementation of systems in line with the APPs. The information is not intended to be a comprehensive list of an APP entity's obligations under the Privacy Act and is not a substitute for an APP entity determining its full obligations under the Privacy Act.

Relevant APP	Key Questions to Consider	Key Actions to Consider
APP 1 – Open and transparent management of personal information	What reasonable steps do we need to take to implement new practices, procedures and systems that will ensure compliance with the new APPs? Do we have a privacy policy? If so, is it up to date? Does it cover the matters listed in the APPs? Is it freely available? What reasonable steps do we need to take to ensure we have practices, procedures and systems in place for handling privacy inquiries and complaints?	Review practices, procedures and systems to ensure compliance with the new APPs. Implement an APP privacy policy. Make APP privacy policy available in an appropriate form and for free. Review practices, procedures and systems for handling privacy inquiries and complaints.
APP 2 – Anonymity and pseudonymity APP 3 – Collection of personal and sensitive information APP 5 – Notification of collection	Do we ensure that sensitive and personal information RTOs are required to collect is collected in accordance with the higher protections in the APPs? How and what matters do we notify individuals about when collecting their personal or sensitive information?	Review collection practices, procedures and systems, including collection notices.
APP 4 – Dealing with unsolicited personal information	Do we receive unsolicited personal information? What are our practices, procedures and systems for dealing with unsolicited information?	Review practices, procedures and systems for dealing with unsolicited information.
APP 6 – Use or disclosure	For what purposes do we use and disclose personal information and sensitive information?	Review practices, procedures and systems for the use and disclosure of personal information and sensitive information.
APP 7 – Direct marketing	Does APP 7 apply to our RTO? If so do we want to use or disclose personal information for the purpose of direct marketing?	Review direct marketing practices, procedures and systems (including whether individuals are provided with an easy way to opt out of receiving direct marketing).
APP 8 – Cross border disclosure	Do we send personal information overseas? Do we have appropriate arrangements with overseas recipients to ensure that personal information that is disclosed overseas is handled in accordance with the APPs?	Review practices, procedures and systems for sending personal information overseas (this may include reviewing outsourcing agreements).
APP 9 – Adoption, use or disclosure of government related identifiers	Does our RTO collect government related identifiers currently? How will we manage the new USI when it is implemented?	Review practices, procedures and systems for the adoption, use or disclosure of government related identifiers.
APP 10 – Quality	What reasonable steps do we need to take to ensure that the personal information we collect, use or disclose is up to date, complete and accurate and relevant for the purpose of the use or disclosure?	Review practices, procedures and systems for ensuring personal information collected, used or disclosed is up to date, complete and accurate and relevant for the purpose of the use or disclosure.