Policy Overview:

This policy is to ensure that ASH Pty. Ltd. (trading as Ashley Institute of Training (ASH)) meets its legal and ethical obligations in regard to the collection, use, storage, security and destruction of personal and sensitive information collected from all stakeholders. ASH will adhere to all legislative requirements as outlined in the Privacy Act 1988, Australian Privacy Principles (and any subsequent amendments) as well as the requirements under the Standards for RTO's 2015.

Objective:

To ensure that ASH, its staff and other stakeholders are aware of the measures in place to ensure the confidentiality and security of their personal and sensitive information and how the information collected will be used.

Scope:

This policy applies to the personal and sensitive information of all stakeholders of ASH.

Staff Responsible:

- National Compliance and Quality Manager
- Operation Managers
- Administration Staff
- Sales Staff
- Training and Assessment Staff

Compliance Standards:

This policy relates to the following Standards for RTO's 2015: 2.2, 3.5, 4.1, 5.1 - 5.3, 5.4, 6.1 - 6.6.

Related Policies/Templates/Documents:

- D-001.2 Student Information Guide
- F-011.2 Code of Conduct for Students
- F-150.2 Code of Conduct for Trainers and Assessors
- F-151.2 Code of Conduct for Administration Staff
- F-152.2 Code of Conduct for Sales Staff
- F-316.2 Student Information Release form
- P-003.2 Record Management and Maintenance Policy
- P-043.2 Issuing AQF Certification Documentation Policy

Definitions:

The **Privacy Act 1988** was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information.

(Source: https://www.oaic.gov.au/privacy/the-privacy-act/)

The **Australian Privacy Principles** (APP) are guidelines that outline the mandatory requirements of the APP, how they interpret the APP's, and matters they may take into account when exercising functions and powers under the Privacy Act 1988. The Australian Privacy Principles are:

APP 1: Open and transparent management of personal information

APP 2: Anonymity and pseudonymity

APP 3: Collection of solicited personal information

APP 4: Dealing with unsolicited personal information

APP 5: Notification of the collection of personal information

APP 6: Use or disclosure of personal information

APP 7: Direct marketing

APP 8: Cross-border disclosure of personal information

APP 9: Adoption, use or disclosure of government related identifiers

APP 10: Quality of personal information

APP 11: Security of personal information

APP 12: Access to personal information

APP 13: Correction of personal information

(Source: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf)

Consent means express or implied consent. The four key elements of consent are:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- The consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.

Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

Informed consent means that an individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. An APP entity should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent. The information should be written in plain English, without legal or industry jargon.

(Source: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf)

Destroying or de-identifying personal information – means that you must take reasonable steps to destroy of de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APP.

Personal information is defined as any information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

(Source: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf)

Sensitive information is a subset of personal information and is defined as:

- Information or an opinion (that is also personal information) about an individual's:
  - Racial or ethnic origin
  - Political opinions
  - Membership of a political association
  - Religious beliefs or affiliations
  - Philosophical beliefs
  - Membership of a professional or trade association
  - Membership of a trade union
  - Sexual orientation or practices, or
  - Criminal record
- Health information about an individual
- Generic information (that is not otherwise health information)
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- Information may be sensitive information where it clearly implies one of these matters. For example, many surnames have a particular racial or ethnic origin, but that alone will not constitute sensitive information that clearly indicates the racial or ethnic origin of an individual with that surname.
- Sensitive information is generally afforded a higher level of privacy protection under the APP's than other personal information. This recognises inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

(Source: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf)

A **Record** is defined in s 3(1) of the Archives Act as 'a document, or an object, in any form (including electronic form) that is, or has been, kept by reason of:

a) Any information or matter that it contains or that can be obtained from it; or
b) Its connection with any event, person, circumstance or thing'.

(Source: https://www.oaic.gov.au/assets/privacy/app-guidelines/app-guidelines-july-2019.pdf)

Notifiable 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.

(Source: https://www.oaic.gov.au/privacy/notifiable-data-breaches/)

Privacy by State

Victoria

Data Protection Act 2014 (VIC): https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/025

Office of the Victorian Information Commissioner: https://ovic.vic.gov.au/

Health Records Act 2001 (Vic): https://www2.health.vic.gov.au/about/legislation/health-records-act

(Source: https://www.oaic.gov.au/privacy/privacy-in-your-state/)

Queensland

Information Privacy Act 2009 QLD: https://www.legislation.qld.gov.au/view/html/inforce/current/act-2009-014

Office of the Information Commissioner Queensland: https://www.oic.qld.gov.au/

(Source: https://www.oaic.gov.au/privacy/privacy-in-your-state/)

Western Australia

Office of the Information Commissioner: https://www.oic.wa.gov.au/en-au/

Freedom of Information Act 1992 (WA): https://www.legislation.wa.gov.au/legislation/statutes.nsf/law_a290.html

(Source: https://www.oaic.gov.au/privacy/privacy-in-your-state/)

Policy

1. Collection of Personal & Sensitive Information

- ASH will collect information from students, staff, other stakeholders in the course of its business operations either in electronic or hard copy format.
- The information collected is for the sole purpose of meeting regulatory, legislative, and contractual requirements relating to training and assessment services that ASH provides.

2. Use & Disclosure of Personal & Sensitive Information

- ASH will ensure that students, staff and other stakeholders are informed about how their personal and sensitive information will be used and for what purpose.
- Personal information such as personal and contact details, course enrolment information may be disclosed when it is necessary to assist a regulator, to meet legislative obligations such as:
    - The Australian Government
    - Australian Apprenticeship Service Network Provider (AASN)
    - National Centre for Vocational Education Research (NCVER)
    - Australian Skills Quality Authority (ASQA)
    - Training Accreditation Council (TAC)
- In accordance with Section 11 of the Student Identifiers Act 2014 Cth (SI Act), ASH will securely store personal information which we collect from the student solely for the purpose of applying for a Unique Student Identifier (USI) on the students behalf. Any person to whom personal information is disclosed, is not permitted to use or disclose the information for a purpose other than the purpose for which the information was gathered.

3. Storage of Personal & Sensitive Information

- ASH will take all reasonable steps to protect and safely store all personal and sensitive information in a central and secure location.
- ASH will ensure that all personal and sensitive information is also saved in the student management system (aXcelerate) which is a Cloud based program.
- ASH does not allow any personal or sensitive information to be stored in any staff members email account and will schedule regular purging of all deleted emails.

4. Data/Information Security

- ASH will schedule automatic purging of all deleted staff emails every 30 days to ensure no personal or sensitive information is held beyond this period.
- ASH will ensure that all personal and sensitive information it holds is protected by:
    - Electronic information held is on a secure server with restricted access for the period of time specified by the regulator, government bodies and any funding contracts.
    - Paper-based files are stored in a secure and locked area with only authorised staff access and information is held for the period specified by the regulator, government bodies and funding contract requirements.

5. Access to Personal & Sensitive Information

- ASH will ensure that students have access to all personal and sensitive information that ASH has collected from them upon request.
- Any student or third-party requesting personal or sensitive information held by ASH will be required to complete a **F-316.2 Student Information Release Form** that **MUST** be signed by the student to allow the information to be released.

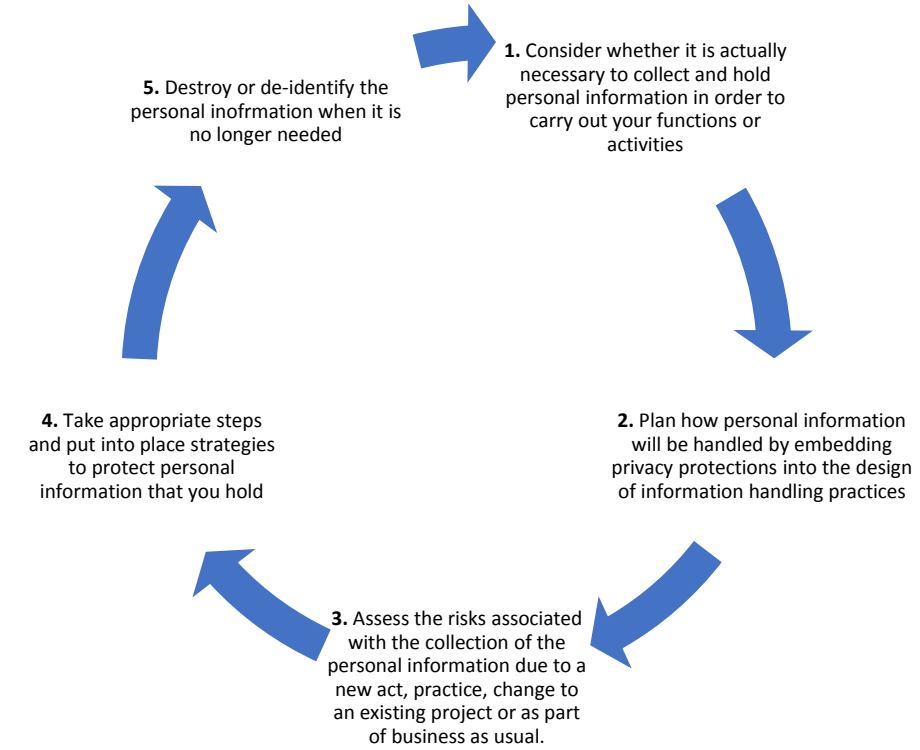
6. Destruction/De-Identifying Personal & Sensitive Information

- ASH will take all reasonable steps to ensure that they destroy or de-identify the personal information they hold once it is no longer needed for any purpose.
- ASH will destroy or de-identify all personal and sensitive information as a key component of their risk mitigation strategy to ensure it complies with all legislative requirements.
- The process of destroying and de-identifying personal and sensitive information will put the information 'beyond use' which includes ensuring there are no backup copies of any kind.

7. Data Breaches

- Under the Notifiable Data Breach scheme, ASH will comply with Australian privacy law by advising the Office of the Australian Information Commissioner (OAIC) of any data breaches within 30 days.
- In the unlikely event of a data breach, ASH will make every effort to reduce the chance of an individual experience of harm.

The Information Life Cycle (Source: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/#s5-destroy-or-de-identify-personal-information)



Privacy and Personal Information Procedure

1. Collection of Personal & Sensitive Information

Action / Task	Responsible	Timeline
Personal / Sensitive Information - Students		
1.1 ASH will collect personal / sensitive information from students as part of the enrolment process.	BDM	Prior to enrolment
1.2 The information collected from students will only include information required by the regulator and any state funding contract.		
1.3 ASH will only use the collected information from any source for the purpose for which it was collected.		
1.4 Students will be advised at the time of enrolment what information needs to be collected, the purpose of collecting the information and that the information will not be used for any other purpose.		
Personal / Sensitive Information - Staff	Operations Manager	As part of the recruitment process
1.5 ASH will collect personal / sensitive information from staff members as part of the recruitment process.		
1.6 The information collected from staff members will only include information required by the Human Resources department and any legislative requirements.		
1.7 ASH will only use collected information from any source for the purpose for which it was collected.		
1.8 Staff will be advised at the time of appointment what information needs to be collected, the purpose of collecting the information and that the information will not be used for any other purpose.		

2. Use & Disclosure of Personal & Sensitive Information

2.1 ASH will ensure that prior to enrolment, students will be informed about why their personal and sensitive information is being collected and how it will be used.	BDM	Prior to enrolment
2.2 ASH will ensure that students are aware that the enrolment collected may be disclosed to the regulator and other bodies to meet legislative obligations. These can include: ▪ The Australian Government ▪ Australian Apprenticeship Service Network Provider (AASN) ▪ National Centre for Vocational Education Research (NCVER) ▪ Australian Skills Quality Authority (ASQA) ▪ Training Accreditation Council (TAC)		

3. Storage of Personal & Sensitive Information

3.1 ASH will take measures to ensure that the secure storage of personal and sensitive information which includes: ▪ All staff responsible for the storage of personal and sensitive information will ensure that it is stored in a secure, central location approved by the Compliance Team in consultation with the Operations Team. ▪ All staff responsible for the storage of personal and sensitive information will ensure that all student information is stored in the student management system (aXcelerate) which is a Cloud based program. ▪ All staff responsible for the storage of personal and sensitive information will ensure that information is only stored for the timeframe specified by the regulator, government bodies and any funding contracts (refer to P-033.2 Records Management Policy & Procedure for further details). ▪ In accordance with Section 11 of the Student Identifiers Act 2014 Cth (SI Act), ASH will securely store personal information which we collect from the student solely for the purpose of applying for a Unique Student Identifier (USI) on the students behalf. Any person to whom personal information is disclosed, is not permitted to use or disclose the information for a purpose other than the purpose for which the information was gathered.	Compliance Team National Systems Manager	Ongoing

4. Data/Information Security

4.1 ASH will take measures to ensure the security of the information it collects and holds by: ▪ Scheduling regular purging of deleted emails every 30 days to ensure no information is held beyond this period in this location. Staff are required to regularly check that any emails in their deleted email folders are no longer required. ▪ All staff responsible for the maintenance of information electronically must ensure that information collected and held by ASH is saved on a secure server in the specified location/s. ▪ All staff responsible for the maintenance of paper-based files are tasked to ensure that these files are always stored in the designated secure and locked area.	National Systems Manager	Every 30 days

5. Access to Personal & Sensitive Information

5.1 Any stakeholder of ASH has access to their personal and sensitive information collected and held by ASH. ***5.2*** Should any stakeholder wish to access their personal or sensitive information, they must first verify their identity and provide written consent by completing the **F-316.2 Student Information Release Form** and sending to the Student Enquiries email address: compliance@ash.edu.au **5.3** Should any third-party request personal or sensitive information held by ASH they will be required to complete **F-316.2 Student Information Release Form** that is signed by the stakeholder giving their permission for the information to be released. **5.4** Where any information has been requested in hard copy/via post, they will be sent to the address held on file for that individual or the address requested by the third-party (such as subpoena documents). **5.5** All requests will be reviewed by the Compliance Team within 15 business days. **5.6** Once approved, the administration staff member can provide the third-party with the requested information. **5.7** If ASH is advised that any personal or sensitive information is incorrect or has changed, an individual can request for this information to be updated by informing ASH in writing and providing proof of the change. This can include although not limited to: ▪ Change of address ▪ Change of name ▪ Change of citizenship ▪ Employment details ▪ If records are found to be incorrect **5.8** There is no charge for this process however where ASH is required to make copies of documents there will be a charge of 20 cents per page. **5.9** Charges will be incurred for re-issuing AQF certification documentation (refer to P-043.2 Issuing AQF Certification Documentation Policy & Procedure). **5.10** The Administration Team must document the process of providing the requested information in the student management system (SMS) in the contact notes.	Compliance Team Administration Staff	At the time of each request

6. Destruction/De-Identifying of Personal & Sensitive Information		
6.1 ASH will take steps to destroy and de-identify information collected and held from all stakeholders by: ▪ ASH will destroy and de-identify information that is deemed to be no longer relevant to the business. ▪ The steps taken by ASH will put the information 'beyond use'	Compliance Team National Systems Manager Relevant staff	Once the information is no longer required
7. Data Breaches		
7.1 If you have identified a data breach you **MUST** report the breach immediately to your direct manager, either: ▪ Operations Manager ▪ General Manager (Training) ▪ Managing Director (ASG)	Operations Manager General Manager (Training) National Systems Manager Managing Director (ASG)	Immediately
7.2 It is the responsibility of Ashley Services Group (ASG) to report all notifiable data breaches to the Office of the Australian Information Commissioner (OAIC) within 30 days of the breach occurring.		Within 30 days of a breach occurring
7.3 A notifiable data breach occurs when: ▪ There is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation holds ▪ This is likely to result in serious harm to one or more individuals **AND** ▪ The organisation has not been able to prevent the likely risk of serious harm with remedial action		
7.4 If a notifiable data breach has occurred, you must notify OAIC and include the following information: ▪ Organisation name ▪ A description of the data breach ▪ The kinds of information involved ▪ Recommendations about the steps individuals should take in response to the data breach	National Systems Manager	
7.5 To submit the abovementioned information, go to: https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/ and complete the online form.	National Systems Manager	As soon as possible

Document Revision History

Version Number	Author	Date Published	Description
2.6	Rebekah Faleafaga	28/01/2020	Updated and revised as per current requirements
2.7	Fiona Dunkerton	06/07/2020	Reviewed and updated to current requirements