PARTNERS TRAINING
Australia

Privacy Policy and Procedures

Partners in Training Australia is committed to maintaining the privacy and confidentiality of its clients, participants, personnel, contractors and other stakeholders. Partners in Training complies with the *Privacy Act 1988* including the 13 Australian Privacy Principles (**APPs**) as outlined in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

As a component of our risk management practices, Partners in Training conducts a Privacy Impact Assessment annually for all operations. Mitigation actions from this risk assessment have been implemented for the management of privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction and de-identification.

Providing an overall framework for our privacy practices, Partners in Training has developed and implemented this Privacy Policy and Procedures.

Partners in Training manages personal information in an open and transparent way. This is evident in the implementation of practices, procedures and systems we outline in this Privacy Policy and Procedures that ensure our compliance with the APPs and any binding registered APP code, and provide suitable procedures for Partners in Training personnel to be able to deal with related enquiries and complaints that may be received from time to time.

The following sections of this Privacy Policy and Procedures outline how we manage personal information.

If you have any queries, concerns or complaints in relation to this Privacy Policy and Procedures please contact:

Partners in Training Privacy Officer

1300 664 601

privacy@pta.edu.au

7 Telford Drive, Shepparton, VIC 3630

Partners in Training reserves the right to amend this Privacy Policy and Procedures at any time and will notify you by posting an updated version of this Privacy Policy and Procedures on Partners in Training's website at http://www.partnersintraining.edu.au/privacy/.

VERSION CONTROL	
Date	**Summary of amendments**
January 2015	Original version
July 2015	Branding updates
May 2016	Branding updates
October 2018	Email address update

Contents

APP 1 – Open and transparent management of personal information

Purposes for information collection, retention, use and disclosure

Partners in Training retains a record of personal information about all individuals with whom we undertake any form of business activity. Partners in Training must collect, hold, use and disclose information from our clients, participants, personnel, contractors and other stakeholders for a range of purposes, including but not limited to:

- Providing services to clients;
- Providing services to participants;
- Managing employees and contractors;
- Promoting products and services;
- Conducting internal business functions and activities; and
- Requirements of stakeholders.

As a government registered training organisation (**RTO**), regulated by the Australian Skills Quality Authority (**ASQA**), Partners in Training 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:

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

It is noted that Partners in Training is also bound by various State Government Acts requiring similar information collection, use and disclosure (particularly *Education Act(s), Vocational Education and Training Act(s) and Traineeship and Apprenticeships Act(s)* relevant to state jurisdictions of Partners in Training's operations). Partners in Training is required to provide the Victorian Government, through the Department of Education and Early Childhood Development, with student and training activity data which may include personal information you provide to us. Information is required to be provided in accordance with the Victorian VET Student Statistical Collection Guidelines (which are available at http://www.education.vic.gov.au/training/providers/rto/Pages/ datacollection.aspx). The Department may use the information provided to it for planning, administration, policy development, program evaluation, resource allocation, reporting and/or research activities. For these and other lawful purposes, the Department may also disclose information to its consultants, advisers, other government agencies, professional bodies and/or other organisations. You may be contacted and requested to participate in a National Centre for Vocational Education Research survey or a Department-endorsed project or audit or review. The *Education and Training Reform Act 2006* requires us to collect and disclose your personal information for a number of purposes including the allocation of a Victorian Student Number and updating your personal information on the Victorian Student Register.

It is further noted that, aligned with these legislative requirements, Partners in Training delivers services through a range of Commonwealth and State Government funding contract agreement arrangements, which also include various information collection and disclosure requirements. For students eligible for VET Student Loans, this includes the collection of personal information for the purpose of assessing a student's entitlement to Commonwealth assistance under the *Higher Education Support Act 2003* and the allocation of a Commonwealth Higher Education Student Support Number (**CHESSN**). Partners in Training will disclose this information to the Commonwealth Department of Industry and Science and the Department of Education and Training for these purposes. These Commonwealth Departments will

store the information securely in the Higher Education Information Management System. These Commonwealth Departments may disclose the information to the Australian Taxation Office.

If you consent to us applying for a Unique Student Identifier (**USI**) on your behalf, the personal information you provide in connection with an application for a USI is collected by the Student Identifier Registrar for the purposes of applying for, verifying and giving a USI, resolving problems with a USI and creating authenticated VET transcripts. The personal information you provide 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 and 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 RTOs 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 for the purpose of creating authenticated VET transcripts, resolving problems with USIs and for the collection, preparation and auditing of national VET statistics; researches for education and training related research purposes; any other person or agency that may be authorised or required by law to access the information; and any entity contractually engaged by the Student Identifier Registrar to assist in the performance of his or her functions in the administration of the USI system. The personal information you provide will not be otherwise disclosed without your consent unless authorised or required by or under law. The Student Identifiers Registrar's Privacy Policy is available at http://usi.gov.au/Pages/privacy-policy.aspx and contains information about how you may access and seek correction of the personal information held about you and complain about a breach of privacy and how such complaints will be dealt with.

Individuals are advised that due to these legal requirements, Partners in Training discloses information held on individuals for valid purposes to a range of entities including:

- Governments (Commonwealth, State or Local);
- Australian Apprenticeships Centres;
- Employers (and their representatives), Job Network Providers, schools, guardians;
- Placement providers; and
- Service providers such as credit agencies, background check providers, tuition assurance schemes, marketing agents, brokers and our HR, IT and legal service providers.

Kinds of personal information collected and held

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

- Name, date of birth and gender;
- Contact details;
- Employment details, including career intentions;
- Education and qualification details;
- Skills and areas of interest;
- Demographic information;
- Course progress and achievement information;
- IP address and dates and times of visits to Partners in Training's websites and social media platforms;
- Survey information and data from events you attend or subscribe to;

- Website data from Partners in Training websites and websites you access whilst using Partners in Training's internet and wireless network services at Partners in Training venues or Partners in Training events; and
- Financial billing information.

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

- Identity details;
- Employee details and HR information;
- Complaint or issue information;
- Disability status and other individual needs;
- Membership of a professional or trade association or trade union;
- Indigenous status;
- Health information;
- Tax file number; and
- Background checks (such as National Criminal Checks or Working with Children Checks).

Where Partners in Training collects personal information from more vulnerable segment of the community (such as children), additional practices and procedures are also followed.

How personal information is collected

Partners in Training's usual 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);
- The use of web based systems (such as online enquiry forms, web portals or internal operating systems);
- The provision of customer service and support, including dealings you may have with Partners in Training personnel;
- Requests for information from Partners in Training, for example to join a mailing list or for brochures;
- Responses to surveys or research;
- The use of social media and other external websites; and
- The use of employment applications.

Partners in Training does receive solicited and unsolicited information from third party sources in undertaking service delivery activities. This may include information from entities such as:

- Governments (Commonwealth, State or Local);
- Australian Apprenticeships Centres;
- Employers (and their representatives), Job Network Providers, schools, guardians;
- Placement providers; and
- Service providers such as credit agencies, background check providers, tuition assurance schemes, marketing agents, brokers and our HR, IT and legal service providers.

How personal information is held

Partners in Training's usual approach to holding personal information includes robust storage and security measures at all times. Information on collection is:

- As soon as practical converted to electronic means;

- In respect of electronically held personal information, stored in secure, password protected systems, such as a financial system, learning management system and/or student management system;
- In respect of paper based personal information, stored in an appropriately secure place to which only authorised individuals have access; 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. Partners in Training ICT systems are hosted with robust internal security to physical server locations and server systems access. 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 at all Partners in Training sites.

Retention and destruction of personal information

Partners in Training maintains a Retention and Disposal Schedule documenting the periods for which personal information records are kept.

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 ASQA, as required by law.

Accessing and seeking correction of personal information

Partners in Training confirms all individuals have a right to request access to their personal information held and to request its correction at any time.

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, Partners in Training will ensure that:

- 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.

The Request for Records Access Procedure is set out in Appendix 1.

The request for records access should be made on Partners in Training's Records Access or Update Request Form and sent to:

Partners in Training Privacy Officer

privacy@pta.edu.au

7 Telford Drive, Shepparton, VIC 3630

Likely overseas disclosures

Partners in Training confirms that individuals' personal information is not disclosed to overseas recipients.

Making this privacy policy and procedures available

Partners in Training provides this Privacy Policy and Procedures free of charge, with all information being publicly available from the Privacy link on our website at http://www.partnersintraining.edu.au/privacy/. This website information is designed to be accessible as per web publishing accessibility guidelines, to ensure access is available to individuals with special needs (such as individuals with a vision impairment).

In addition, this Privacy Policy and Procedures is:

- Prominently displayed at each of Partners in Training's premises;
- Included within our Student Handbook and HR Induction Manual;
- Noted within the text or instructions at all information collection points (such as informing individuals during a telephone call of how the policy may be accessed, in cases where information collection is occurring); and
- Available for distribution free of charge on request, as soon as possible after the request is received, including in any particular format requested by the individual as is reasonably practical.

If, in the unlikely event the Privacy Policy and Procedures is not able to be provided in a particular format requested by an individual, we will explain the circumstances around this issue with the requestor and seek to ensure that another appropriate method is provided.

Review and update of this Privacy Policy and Procedures

Partners in Training reviews this Privacy Policy and Procedures:

- On an ongoing basis, as suggestions or issues are raised and addressed, or as government required changes are identified;
- Through our internal audit processes on at least an annual basis;
- As a part of any external audit of our operations that may be conducted by various government agencies as a part of our registration as an RTO or in normal business activities; and
- Within 8 weeks of each and every complaint investigation process where the compliant is related to a privacy matter.

Where this Privacy Policy and Procedures is updated, changes to the policy are widely communicated to stakeholders through internal personnel communications, meetings, training and documentation, and externally through publishing of the policy on Partners in Training's website and other relevant documentation (such as our Student Handbook) for clients and participants.

Privacy complaints procedure

Partners in Training is committed to providing a fair and responsive system for handling and resolving complaints.

If an individual feels that Partners in Training has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. We encourage individuals to discuss the situation with their Partners in Training representative in the first instance before making a complaint.

The Privacy Complaints Procedure is set out in Appendix 2.

APP 2 – Anonymity and pseudonymity

Partners in Training provides individuals with the option of not identifying themselves, or of 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 individual's information is not required to complete a request.

Individuals may deal with us by using a name, term or descriptor that is different to the individual's actual name wherever possible. This includes using generic email addresses that do not contain an individual's actual name, or generic user names when individuals may access a public component of our website or enquiry forms.

Partners in Training only stores and links pseudonyms to individual personal information in cases where this is required for service delivery (such as system login information) or once the individual's consent has been received.

Individuals are advised of their opportunity to deal anonymously or by pseudonym with us where these options are possible.

Requiring identification

Partners in Training must require and confirm identification in service delivery to participants for nationally recognised course programs. We are authorised by Australian law to deal only with individuals who have appropriately identified themselves. That is, it is a Condition of Registration for all RTOs under the *National VET 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.

There are also other 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.

APP 3 – Collection of solicited personal information

Partners in Training 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 earlier in this policy.

All information we collect is collected only by lawful and fair means.

We only collect solicited information directly from the individual concerned, unless it is unreasonable or impracticable for the personal information to only be collected in this manner or the individual has given their consent to collect solicited information from third parties.

APP 4 – Dealing with unsolicited personal information

Partners in Training 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 Privacy Policy and Procedures.

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).

APP 5 – Notification of the collection of personal information

Whenever Partners in Training collects personal information about an individual, we take reasonable steps to notify the individual of the details of the information collection or otherwise ensure the individual is aware of those matters. This notification occurs at or before the time of collection, or as soon as practicable afterwards.

Our notifications to individuals on data collection include:

- Partners in Training'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.
- A link to this Privacy Policy and Procedures on our website or explain how it may be accessed; and
- Advice that this Privacy Policy and Procedures contains information about how the individual may access and seek correction of the personal information held by us; and how to complain about a breach of the APPs, or any registered APP code, and how we will deal with such a complaint.

Where possible, we ensure that 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 Partners in Training collects personal information from another organisation, we:

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

APP 6 – Use or disclosure of personal information

Partners in Training 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.

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

If Partners in Training uses or discloses personal information in accordance with an 'enforcement related activity' we 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; and
- The basis for our reasonable belief that we were required to disclose the information.

APP 7 – Direct marketing

Partners in Training does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, unless:

- We have obtained the consent of the individual;
- 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 each of our direct marketing communications, Partners in Training provides a prominent statement that the individual may request to opt out of future communications, and how to do so.

An individual may also request us 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. We comply with any request by an individual promptly and undertake any required actions for free.

We also, on request, notify an individual of our source of their personal information used or disclosed for the purpose of direct marketing unless it is unreasonable or impracticable to do so.

APP 8 – Cross-border disclosure of personal information

Before Partners in Training discloses personal information about an individual to any overseas recipient, we undertake reasonable steps to ensure that the recipient does not breach any privacy matters in relation to that information.

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

Partners in Training 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.

APP 10 – Quality of personal information

Partners in Training takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. We also take 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. This is particularly important when:

- We initially collect the personal information; and

- We use or disclose personal information.

We take steps to ensure personal information is factually correct. In cases of an opinion, we ensure information takes into account competing facts and views and makes an informed assessment, providing it is clear this is an opinion. Information is confirmed up-to-date at the point in time to which the personal information relates.

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;
- 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.

APP 11 – Security of personal information

Partners in Training takes active measures to consider whether we are able to retain personal information we hold, and also 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.

We 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 Partners in Training offices and work areas is limited to our personnel only - visitors to our premises must be authorised by relevant personnel and are accompanied at all times. With regard to any information in a paper based form, we maintain storage of records in an appropriately secure place to which only authorised individuals have access.

Regular staff training and information bulletins are conducted with Partners in Training personnel on privacy issues, and how the APPs apply to our practices, procedures and systems. Training is also included in our personnel induction practices.

We conduct ongoing internal audits (at least annually and as needed) of the adequacy and currency of security and access practices, procedures and systems implemented.

If Partners in Training determines that there has been a data breach, it will implement the Data Breach Response Plan set out in Appendix 3.

APP 12 – Access to personal information

Where Partners in Training holds personal information about an individual, we provide that individual access to the information on their request. In processing requests, we:

- Ensure 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.
- Respond 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.
- Provide information access free of charge.

APP 13 – Correction of personal information

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

Individual requests

On an individual's request, we:

- 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 we refuse to update personal information, we:

- 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.

The Request for Records Update Procedure is set out in Appendix 4.

The request for records update should be made on Partners in Training's Records Access or Update Request Form and sent to:

Partners in Training's Privacy Officer

privacy@pta.edu.au

7 Telford Drive, Shepparton, VIC 3630

Correcting at Partners in Training's initiative

We take 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.

Appendix 1 – Request for records access procedure

Individuals or third parties may at any stage request access to records held by Partners in Training relating to their personal information. The following procedure is followed on each individual request for access.

1. A request for access is provided by the requestor, with suitable information provided to be able to:
    (a) Identify the individual concerned;
    (b) Confirm their identity; and
    (c) Identify the specific information that they are requesting access to.

A request should be made using Partners in Training's Records Access or Update Request Form.

2. Upon receiving a request for access, Partners in Training then:
    (a) Confirms the identity of the individual or party requesting access;
    (b) Confirms that this individual or party is appropriately authorised to receive the information requested;
    (c) Searches the records that we possess or control to assess whether the requested personal information is contained in those records; and
    (d) Collates any personal information found ready for access to be provided.

Partners in Training personnel must be satisfied that a request for personal information is made by the individual concerned, or by another person who is authorised to make a request on their behalf. The minimum amount of personal information needed to establish an individual's identity is sought, which is generally an individual's name, date of birth, last known address and signature.

When meeting the requesting party in person, identification may be sighted.

If confirming details over a telephone conversation, questions regarding the individual's name, date of birth, last known address or service details may be confirmed before information is provided.

3. Once identity and access authorisation is confirmed, and personal information is collated, access is provided to the requestor within 30 calendar days of receipt of the original request. We 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, we consult with the requestor to ensure a format is provided that meets the requestor's needs.

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

Appendix 2 – Privacy complaints procedure

Individuals or third parties may at any stage make a complaint in relation to Partners in Training's handling, use or disclosure of an individual's personal information. The complaints handling process is as follows.

1. The individual should make the complaint including as much detail about the issue as possible, in writing to:

   Partners in Training Privacy Officer

   privacy@pta.edu.au

   7 Telford Drive, Shepparton, VIC 3630

2. Partners in Training will investigate the circumstances included in the complaint and respond to the individual as soon as possible (and within 30 calendar days) regarding its findings and actions following this investigation.

3. If the individual is still not satisfied after receiving and considering this response, they may escalate their complaint directly to the Information Commissioner for investigation:

   Office of the Australian Information Commissioner (**OAIC**)

   www.oaic.gov.au

   Phone: 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.

4. Alternatively, if the complaint relates to a non-privacy matter, or should individuals choose to do so, a complaint may also be made through Partners in Training's general complaint procedure, and if you believe that the complaint is not satisfactorily resolved by Partners in Training, a complaint may also be lodged with the ASQA complaints handing service for complaints against RTOs:

   Australian Skills Quality Authority

   www.asqa.gov.au

   Phone: 1300 701 801

Appendix 3 – Data breach response plan

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse.

Data breaches when they occur can be caused by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals and organisations. Each breach will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

There are four key steps to consider when responding to a breach or suspected breach:

1. Contain the breach and do a preliminary assessment.
2. Evaluate the risks associated with the breach.
3. Notification.
4. Prevent future breaches.

When dealing with any breach, some key items to consider include:

- Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.
- Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- Steps 1, 2 and 3 should be undertaken promptly. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- The decision on how to respond should be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined.

RESPONDING TO A DATA BREACH	
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:

RESPONDING TO A DATA BREACH	
	1. Legal/contractual obligations to notify. 2. 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.

Appendix 4 – Request for records update procedure

Individuals or third parties may at any stage request that their records held by Partners in Training relating to their personal information be updated. The following procedure is followed on each individual request for records updates.

1. A request for records update is provided by the requestor, with suitable information provided to be able to:
   (a) Identify the individual concerned;
   (b) Confirm their identity; and
   (c) Identify the specific information that they are requesting be updated on their records.
   A request should be made using Partners in Training's Records Access or Update Request Form.
2. Upon receiving a request for records update, Partners in Training then:
   (a) Confirms the identity of the individual or party to whom the record relates;
   (b) Searches the records that we possess or control to assess whether the requested personal information is contained in those records; and
   (c) Assesses the information already on record, and the requested update, to determine whether the requested update should proceed.

Partners in Training personnel assess the relevant personal information we hold, and the requested updated information, to determine which version of the information is considered accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

This may include checking information against other records held by us, or within government databases, in order to complete an assessment of the correct version of the information to be used.

3. Once identity and information assessment is confirmed, personal information is:
   (a) Updated, free of charge, within 14 calendar days of receipt of the original request; and
   (b) Notified to any third parties of corrections made to personal information, if this information was previously provided to these parties.
4. If the identity of the individual cannot be confirmed, or there is another valid reason why Partners in Training is unable to update the personal information, written notice of the refusal to update records will be provided to the requestor in writing, free of charge, within 14 calendar days.

   Our notification will include the reasons for the refusal and the complaint mechanisms available to the individual.

5. Upon request by the individual whose correction request has been refused, we 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, free of charge, to all personal information relevant across Partners in Training systems within 30 calendar days of receipt of the statement request.