Privacy Policy and Procedures

PURPOSE

Blue Dog Training is committed to maintaining the privacy and confidentiality of its personnel, student and stakeholder records.

Blue Dog 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.*

So as to provide an overall framework for our privacy practices - including how to deal with related inquiries and complaints that may be received from time to time - Blue Dog Training has developed and implemented this policy.

This policy is designed to maintain requirements with additional state jurisdictional requirements including:

- ✓ *Privacy and Personal Information Protection Act 1998 (NSW);*
- ✓ *Information Privacy Act 2009(QLD);*

PRINCIPLES

Blue Dog Training manages personal information in an open and transparent way.

This is evident in the implementation of practices, procedures and systems as outlined in this policy, that ensure our compliance with the APPs and any binding registered APP code, and provide suitable procedures for Blue Dog Training personnel to be able to deal with related inquiries and complaints that may be received from time

AUSTRALIAN PRIVACY PRINCIPLES (APP)

The following sections of this policy outline how Blue Dog Training as a registered training organisation (RTO) ensures its operations are compliant with the *Privacy Act 1988 (Cth)* and APP requirements.

Australian Privacy Principle 1:	**Open and transparent management of personal information**

The objective of this principle is to ensure that Blue Dog Training manages personal information in an open and transparent way. This enhances the accountability of Blue Dog Training for personal information handling practices and can build community trust and confidence in these practices.

Blue Dog Training retains a record of personal information about all individuals with whom it undertakes any form of business activity. Blue Dog Training collects, holds, uses and discloses information from clients and stakeholders for a range of purposes, including but not limited to:

- ✓ Providing services to clients and students
- ✓ Managing employee and contractor teams
- ✓ 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) Blue Dog 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:

- ✓ *Student Identifiers Act 2014 (Cth)*
- ✓ *Standards for Registered Training Organisations (RTOs) 2015;* and
- ✓ *Data Provision Requirements 2012 (Cth).*

Blue Dog Training is also bound by various State Government Acts requiring similar information collection, use and disclosure (particularly *Education Act(s), Vocational Education & Training Act(s) and Traineeship & Apprenticeships Act(s)* relevant to state jurisdictions of Blue Dog Training operations).

Aligned with these legislative requirements, Blue Dog Training delivers services through a range of Government funding contract agreement arrangements, which also include various information collection and disclosure requirements.

Individuals are advised that due to these legal requirements, Blue Dog Training discloses information held on individuals for valid purposes to a range of entities including but not limited to:

- ✓ Governments (Commonwealth, State or Local)
- ✓ Australian Apprenticeships Support Networks (AASNs)
- ✓ Employers (and their representatives), Job Network Providers, schools, guardians; and
- ✓ Service providers such as credit agencies and background check providers.

1. Kinds of personal information collected and held

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

- ✓ Contact details
- ✓ Employment details
- ✓ Educational background
- ✓ Demographic Information
- ✓ Course progress and achievement information; and
- ✓ Financial billing information.

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

- ✓ Identity details
- ✓ Employee details & HR information
- ✓ Complaint or issue information
- ✓ Disability status & other individual needs
- ✓ Indigenous status; and
- ✓ Background checks (such as National Criminal Checks or Working with Children checks).

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

Refer to the Blue Dog Training Child Safety Policy for further information.

2. How personal information is collected

Blue Dog 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) and the use of web-based systems (such as online enquiry forms, web portals or internal operating systems).

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

- ✓ Governments (Commonwealth, State or Local)
- ✓ Australian Apprenticeships Support Networks (AASNs)
- ✓ Employers (and their representatives), Job Network Providers, schools, guardians; and
- ✓ Service providers such as credit agencies and background check providers.

3. How personal information is held

Blue Dog Training's 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
- ✓ Stored in secure, password protected systems, such as financial system, learning management system and student management system; 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.

Blue Dog Training ICT systems are hosted in highly secured data centres (undisclosed locations, with armed security. Blue Dog Training has robust access protection with passwords and private keys for authentication. On top of this, the infrastructure sits behind firewalls and only whitelisted IP addresses are allowed to connect. 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 Blue Dog Training sites.

Individual information held across systems is linked through a Blue Dog Training allocated identification number for each individual.

4. Retention and Destruction of Information

The process by which Blue Dog Training collects, manages, maintains and disposes of student, personnel, finance and other records is outlined in the Blue Dog Training Records Management Policy.

Specifically, for RTO related records, in the event of Blue Dog Training ceasing to operate the required personal information on record for individuals undertaking nationally recognised training would be transferred to the Australian Skills Quality Authority, as required by law.

5. Accessing and seeking correction of personal information

Blue Dog Training confirms all individuals have a right to request access to their personal information held and to request its correction at any time. In order to request access to personal records, individuals are in the first instance to make contact with their trainer.

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 Support Networks, Governments (Commonwealth, State or Local) and various other stakeholders.

In all cases where access is requested, Blue Dog Training will ensure:

- ✓ 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.

6. Complaints about a breach of the APPs or a binding registered APP code

If an individual feels Blue Dog Training may have breached one of the APPs they should follow the complaints procedure which forms part of this policy.

7. Likely overseas disclosures

It is highly unlikely Blue Dog Training will be required to disclose personal information to overseas recipients.

If these situations do arise Blue Dog Training will confirm at that time that individuals' personal information is likely to be disclosed to overseas recipients, for internal business activity purposes. Any type of personal information held by Blue Dog Training (as listed in this policy) may be included in these disclosures.

8. Making our Privacy Policy available

Blue Dog Training provides this policy free of charge, with all information being publicly available from the Privacy link on our website at www.bluedogtraining.com.au . This website information is designed to be accessible as per web publishing accessibility guidelines, to ensure access is available to individuals with special needs.

In addition, this Policy is:

- ✓ Available to staff at each Blue Dog Training premises
- ✓ Included in the Blue Dog Training Student Handbook
- ✓ Noted with the text or instructions at all information collection points (such as informing individuals during a telephone call on how the policy may be accessed, in cases where information collection is occurring)
- ✓ 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 Policy is not able to be provided in a particular format requested by an individual, Blue Dog Training will discuss the circumstances around this issue with the requester and seek to ensure that another appropriate method is provided, if at all possible.

9. Review and Update of this policy

Blue Dog Training will review this policy:

- ✓ 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
- ✓ As a component of each and every complaint investigation process where the compliant is related to a privacy matter.

Where this Policy is updated, changes to the Policy will be communicated to stakeholders through internal personnel communications, meetings, training and documentation, and externally through publishing of the policy on the Blue Dog Training website and other relevant documentation for students.

Australian Privacy Principle 2: Anonymity and Pseudonymity

This principle provides that individuals must have an option of not identifying themselves or using a pseudonym when dealing with a registered training organisation (RTO) in relation to a particular matter.

The principle does not apply in relation to the following:

1. Requiring identification – Required of authorised by law

RTOs in service delivery to clients for nationally recognised course programs are required and authorised by Australian law to deal with individuals who have identified themselves. That is, it is a condition of Registration for all RTOs under the *National Vocational Education and Training Regulator Act 2011* that RTOs collect and report on the *Australian Vocational Education and Training Management of Information Statistical Standard* (AVETMISS) data for all participants enrolled in nationally recognised training programs. RTOs must ensure however that the collection of personal information does not go beyond the requirements of law. For example, the legal requirement may not extend to the requirement to collect an individual's 'next of kin' details.

2. Requiring identification – Impracticability

This principle provides that an individual may not have the option of dealing anonymously or by pseudonym with an RTO if it is impractical for the RTO to deal with individuals who have not identified themselves. The following are examples of where it may be impractical to deal with an individual who is not identified:

- ✓ Dispute resolution – it may be impractical to investigate and resolve an individual's particular complaint about how their case was handled unless the complainant provides their name or similar information
- ✓ Eligibility for government subsidies or support – in responding to an individual's course inquiries and government subsidy support that may be available, the RTO may not be able to provide that information without knowing the requester's identity and individual characteristics.

Blue Dog Training acknowledges that anonymity and pseudonymity are important privacy concepts. They enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others. Whenever practical Blue Dog Training provides individuals with the option of not identifying themselves, or of using a pseudonym.

a) Anonymity

Anonymity requires that an individual may deal with Blue Dog Training without providing any personal information or identifiers where possible. In such cases Blue Dog Training should not be able to identify the individual at the time of the dealing or subsequently.

Examples of anonymous dealings include an unidentified individual telephoning Blue Dog Training to inquire generally about its courses or services

b) Pseudonymity

Pseudonymity requires that an individual may deal with Blue Dog Training by using a name, term or descriptor that is different to the person's actual name. Examples include an email address that does not contain the individual's actual name, or generic user names in situations where individuals may access a public component of our website or enquiry forms. The use of a pseudonym does not necessarily mean that an individual cannot be identified. The individual may choose to divulge their identity, or to volunteer personal information necessary to implement a particular transaction where required practically for service delivery or by law.

Personal information should only be linked to a pseudonym if it is required or authorised by law, it is impractical for the RTO to act differently, or the individual has consented to providing or linking the additional information. Blue Dog Training only stores and links pseudonyms to individual personal information in cases where this is required for services delivery (such as system login information) or once the individual's consent has been received.

Blue Dog Training advises individuals of their opportunity to deal anonymously or by pseudonym with us where these options are possible.

Australian Privacy Principle 3: Collection of Solicited Personal Information

Under this principle an RTO solicits personal information if it explicitly requests another organisation to provide personal information or it takes active steps to collect personal information. Examples of solicited information includes:

- ✓ Information provided by an individual or another party in response to requests. This may include information from an individual's parents, employers, schools, Australian Apprentices Support Network, or from government websites and registers.
- ✓ A completed form or application submitted by an individual
- ✓ A complaint letter sent in response to a general invitation on the RTO's website to individuals to complain to the RTO
- ✓ An employment application sent in response to a job advertisement published by the RTO
- ✓ A form completed to enter a competition conducted by the RTO
- ✓ An entry in the RTO's office visitors book and
- ✓ A record of a credit card payment.

This principle deals with two (2) aspects of collecting solicited personal information:

- ✓ When an RTO can collect personal information and
- ✓ How an RTO must collect personal information

In response to the requirements of this principle, Blue Dog Training:

- ✓ only collects personal information that is reasonably necessary for one or more of its functions or activities
- ✓ only collects sensitive information in cases where the individual consents to the sensitive information being collected, unless an exception applies
- ✓ only collects information by lawful and fair means
- ✓ only collects solicited information directly from the individual concerned, unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

Australian Privacy Principle 4: Dealing with Unsolicited Personal Information

This principle outlines the steps an RTO must take if it receives unsolicited personal information. Unsolicited personal information is information received- by an RTO that has not been requested by that RTO.

Blue Dog Training may from time to time receive unsolicited personal information. Where this occurs Blue Dog Training promptly reviews 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, Blue Dog Training may hold, use and disclose the information appropriately as per the practices outlined in this policy.

Where Blue Dog Training could not have collected this information (by law or for a valid business purpose) Blue Dog Training will immediately destroy or de-identify the information (unless it would be unlawful to do so).

Australian Privacy Principle 5: Notification of the Collection of Personal Information

This principle requires an RTO that collects personal information about an individual to take reasonable steps to notify the Whenever Blue Dog Training collects personal information about an individual, Blue Dog Training takes reasonable steps to notify the individual of the details of the information collection or

otherwise ensures the individual is aware of those matters. This notification occurs at or before the time of collection, or as soon as practicable afterwards.

Blue Dog Training notifications to individuals on data collection include:

- ✓ Blue Dog 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 policy on the Blue Dog Training website or explain how it may be accessed; and
- ✓ Advice that this Policy contains information about how the individual may access and seek correction of the personal information held by Blue Dog Training and how to complain about a breach of the APPs and how Blue Dog Training will deal with such a complaint.

Where possible, Blue Dog Training will ensure 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 Blue Dog Training collects personal information from another organisation, Blue Dog Training will:

1. Confirm whether the other organisation has provided the relevant notice above to the student; 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.

Australian Privacy Principle 6: Use or disclosure of personal information

Blue Dog 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 a written note of use or disclosure for this secondary purpose

If Blue Dog Training uses or discloses personal information in accordance with an 'enforcement related activity' (as defined by the APPs, Office of the Australian Information Commissioner) Blue Dog Training 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;
- ✓ The basis for our reasonable belief that we were required to disclose the information.

Australian Privacy Principle 7: Direct Marketing

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

- ✓ The personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing; or
- ✓ The personal information has been collected from a third party, or from the individual directly, but the individual does not have a reasonable expectation that their personal information will be used for the purpose of direct marketing; and
- ✓ We provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

On all direct marketing communications, Blue Dog 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 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. Blue Dog Training will promptly comply with any request by an individual and undertake any required actions for free. On request, Blue Dog Training will 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.

Australian Privacy Principle 8: Cross-border disclosure of personal information

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

Australian Privacy Principle 9: Adoption, use or disclosure of government related identifiers

Blue Dog 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.

Australian Privacy Principle 10: Quality of personal information

Blue Dog Training takes reasonable steps to ensure that the personal information it collects is:

- ✓ Accurate
- ✓ up-to-date and
- ✓ complete.

Blue Dog Training also takes reasonable steps to ensure that the personal information we use or disclose is, also relevant for the purpose or disclosure.This is particularly important:

- ✓ When information is initially collected and

- ✓ When personal information is used or disclosed.

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
- ✓ Providing individuals with a simple means to review and update their information on an on-going basis through our online portal
- ✓ 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 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.

Australian Privacy Principle 11: Security of personal information

Blue Dog 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.

Blue Dog Training will destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

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

Staff training and information sessions are conducted with Blue Dog Training personnel on privacy issues, and how the APPs apply to our practices, procedures and systems. Training is also included in the Blue Dog Training personnel induction practices.

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

Australian Privacy Principle 12: Access to personal information

Where Blue Dog Training holds personal information about an individual, Blue Dog Training provides that individual access to the information on their request. In processing requests, Blue Dog Training:

- ✓ Ensures 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;
- ✓ Responds 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.
- ✓ Provides information access free of charge.

Australian Privacy Principle 13:	Correction of personal information

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

a) Individual Requests

On (written) request from an individual Blue Dog Training will:

- ✓ 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 Blue Dog Training refuses to update personal information, Blue Dog Training will:

- ✓ 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.

b) Correcting at Blue Dog Training's initiative

Blue Dog Training will take reasonable steps to correct personal information in cases where Blue Dog Training is 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.

PROCEDURE – Request for Records access

Individuals or third parties may at any stage request access to records held by Blue Dog 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 requester, with suitable information provided to be able to:
   - ✓ Identify the individual concerned
   - ✓ Confirm their identity; and
   - ✓ Identify the specific information that they are requesting access to.
2. This request is to be made in writing, and in the first instance should be made to the individual's trainer.
3. Upon receiving a request for access, Blue Dog Training will:
   - ✓ Confirm the identity of the individual or party requesting access
   - ✓ Confirm that this individual or party is appropriately authorised to receive the information requested
   - ✓ Search the Blue Dog Training records to assess whether the requested personal information is contained in those records; and
   - ✓ Collate any personal information found ready for access to be provided.
4. Once identity and access authorisation is confirmed, and personal information is collated, access is provided to the requester within 30 calendar days of receipt of the original request.

Blue Dog Training 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, Blue Dog Training will consult with the requester to ensure a format is provided that meets the requester's needs.

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

PROCEDURE – Request for Records Update

Individuals or third parties may at any stage request their records (held by Blue Dog Training and 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 requester, with suitable information provided to be able to:
   - ✓ Identify the individual concerned
   - ✓ Confirm their identity; and
   - ✓ Identify the specific information that they are requesting be updated on their records.

   This request must be in writing.
2. Upon receiving a request to update records Blue Dog Training then:
   - ✓ Confirms the identity of the individual or party to whom the record relates
   - ✓ Searches the records that Blue Dog Training possesses or controls to assess whether the requested *personal information* is contained in those records; and
   - ✓ Assesses the information already on record, and the requested update, to determine whether the requested update should proceed. This may include checking information against other records held by Blue Dog training or within government databases in order to complete an assessment of the correct version of information to be used.
3. Once identity and information assessment is confirmed, personal information is:
   - ✓ Updated, free of charge, within 14 calendar days of receipt of the original request; and
   - ✓ 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 Blue Dog Training is unable to update the personal information, refusal to update records will be provided to the requester in writing, free of charge, within 14 calendar days. The Blue Dog Training 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, Blue Dog Training 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 Blue Dog Training systems within 30 calendar days of receipt of the statement request.

PROCEDURE – Complaints Management

If an individual feels Blue Dog Training has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. Blue Dog Training encourages individuals to discuss the

situation with their Blue Dog Training trainer (or other representative) in the first instance, before making a complaint.

Privacy related complaints are managed through the Blue Dog Training Complaints and Appeals Policy.

If after following that process the individual is still not satisfied they can escalate their complaint directly to the Office of the Australian Information Commissioner (OAIC) for investigation. Website address www.oaic.gov.au or phone number 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.

A complaint may also be lodged with the Australian Skills Quality Authority (ASQA) complaints handing service for complaints against RTOs at either the website www.asqa.gov.au or phone 1300 701801.

PROCEDURE – Data Breach Response

Blue Dog Training recognizes that 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.

Blue Dog Training will deal with each breach 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.

When dealing with any breach, Blue Dog Training will:

- ✓ Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.
- ✓ Acknowledge that breaches which may initially seem immaterial may be significant when their full implications are assessed.
- ✓ Respond promptly. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- ✓ Blue Dog Training acknowledges 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.

The following steps for the basis for the preparation of a Blue Dog Training Data Breach Response Plan.

Responding to a data breach *(Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse.)*	
Step 1: Contain	Contain the breach and make a preliminary assessment: √ Take immediate steps to contain breach. √ Identify and designate a 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. √ Determine if notifications should occur. Where there is a real risk of serious harm, notification may enable individuals to take steps to avoid or mitigate harm. Consider:

	• Legal/contractual obligations to notify. • Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities. √ Process of notification: • When? As soon as possible. • How? Direct contact if possible (mail/phone). • Who? The affected individual. • What? Description of the breach, type of personal information involved, steps to help mitigate, contact details for information and assistance, other actions underway √ Should others be notified, for example • 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.

FURTHER INFORMATION

- ✓ *APP Quick Reference Tool* - http://oaic.gov.au/privacy/privacy-resources/privacy-guides/app-quick-reference-tool
- ✓ *Australian Privacy principles* - https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles.
- ✓ *APP and National Privacy Principles – A Comparison Guide* - http://oaic.gov.au/privacy/privacy-resources/privacy-guides/australian-privacy-principles-and-national-privacy-principles-comparison-guide
- ✓ *OAIC APP Guidelines* - http://oaic.gov.au/privacy/applying-privacy-law/app-guidelines/
- ✓ *OAIC Privacy Guides* - http://oaic.gov.au/privacy/privacy-resources/privacy-guides/
- ✓ *Privacy Act 1988* - http://www.comlaw.gov.au/Series/C2004A03712
- ✓ *Privacy Impact Assessment Guide* - http://oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide
- ✓ *Office of the Australian Information Commissioner* - http://www.oaic.gov.au