Privacy Policy and Procedure

Policy and Procedure Name	Privacy Policy and Procedure
Version	2.0
Approved By	Chief Executive Officer
Date Approved	7/06/2016
Review Date	3/05/2017

1. Purpose and Scope

BSI Learning in accordance with the Australian Privacy Principles has a commitment to ensuring that all reasonable steps are taken to protect the privacy of its consumers and staff. The following policy and procedure outlines how personal information is collected, used, disclosed, stored, destroyed.

The Privacy policy and procedure applies to staff, students, employers, clients and potential consumers and is used throughout all aspects of business operations.

The following policy and procedure should be read in conjunction with the *"Record Retention Policy and Procedure*", *"Engagement and Monitoring of Third Party Providers Policy and Procedure"* and the organisations "*Complaints and Appeals Policy and Procedure*".

2. Abbreviations / Definitions

AVETMISS	The agreed national data standard for the collection, analysis and reporting of vocational education and training information.[1]
Data breach	Where personal information is held by an organisation and is lost or subjected to unauthorised access, use, modification, disclosure or other misuse[2].
Personal information	Types of information that are specific to an individual for example name, address, contact or bank account details.[3]
OAIC	Office of the Australian Information Commissioner
Sensitive information	A type of personal information that is sensitive in its nature – for example race or ethnic origin, political opinion, religious belief or affiliation, medical history or criminal record.[4]

[1] NCVER (2014) Glossary of VET
[2] Office of the Australian Information Commissioner (2014) Australian Privacy Principles Guidelines
[3] Office of the Australian Information Commissioner (2014) Australian Privacy Principles Guidelines
[4] Office of the Australian Information Commissioner (2014) Australian Privacy Principles Guidelines

3. Policy and Procedure

In order to deliver a high quality education service BSI Learning is required to collect a variety of personal information from both consumers and staff members. Where personal and sensitive information is collected it is stored, disclosed and destroyed in accordance with the Australian Privacy Principles.

The following principles underpin the organisations privacy policy and procedure;

- Personal information is protected by the Privacy Act 1988.
- BSI Learning takes all reasonable steps required to protect and maintain personal and sensitive information.
- A robust governance framework is used to assess, plan, implement and review the protection of personal information against misuse, loss, inappropriate access, and inappropriate disclosure.
- Prior to the collection of personal and sensitive information the individual is told what information is to be collected and stored, the purpose of collection, if this information is to be disclosed to a third party and/or under what circumstances disclosure may occur.
- Once the individual is well informed consent is obtained for the collection of information.
- Personal and sensitive information is used only for the purpose of its collection and by staff who require the information in order to complete their duties.
- Individuals have access to their information when required and without charge.
- Personal information is stored in either an electronic or hardcopy format.
- Security measures such as unique password requirements and restricted file access are used to maintain and protect students/clients and employee's privacy.
- BSI Learning will only *disclose* personal information to a third party where written consent has been obtained from the individual.
- Where BSI Learning receives unsolicited information it is either destroyed or de-identified
- The Privacy policy and procedure is publically available on the website and a synopsis can be found in the student's handbook. More information on the Privacy Act can be found at www.privacy.gov.au

3.1 Types of information collected and held

Personal and sensitive information is routinely collected from staff and consumers for the purpose of either employment or enrolment.

i. Information collected for the purpose of employment

- Name
- Address
- Contact detail
- Emergency contact
- Employment history
- Qualifications
- Verification documentation and evidence
- Registration/ Licensing documentation
- Recent professional development activities
- Reference checks
- Vulnerable person checks – National Police Clearance Checks, Working with Children Checks
- Proof of identity – 100 Point ID check
- Superannuation details
- Tax File Number
- Insurance documentation
- Bank details

ii. Information collected for the purpose of enrolment in a qualification or program

- Name
- Address
- Contact details
- Emergency contact
- Employment history / status
- Centrelink information, government allowances
- Citizenship, Residency and Visa status and information
- Language, literacy and numeracy assessments
- Indigenous status
- Proof of identity – 100 Point ID check
- Unique Student Identifier (USI)
- Disability / special need requirements
- Schooling / qualifications completed
- Verification documentation and evidence
- Vulnerable person checks – National Police Clearance Checks, Working with Children Checks
- Fee payment information- e.g. credit card information, banking details

3.2 How personal information is collected and stored

Individuals may disclose information over the telephone, via email, in person and by the completion of relevant forms. Only information disclosed by the individual is used in the collection of information. Prior to the collection of personal information, the individual is told what information is to be collected and stored, the purpose of collection, if this information is to be disclosed to a third party and/or under what circumstances disclosure may occur.

Written and/or verbal consent is obtained prior to collection of personal information and stored appropriately (e.g. in the students/employee file or on the student management system). For individuals under 18 years of age parent/guardian consent is sought/required.

The types of information collected or disclosed by the individual will vary depending on the method of collection, the purpose of that collection and the individual disclosing the information.

Forms used by BSI Learning to collect personal information from students include;

- Enquiry forms
- Application forms
- Enrolment forms
- Application for credit transfer form
- Assessment tasks submission forms
- Training plans/ Individualised learning and assessment plans

Documentation used by BSI Learning to collect personal information from staff include;

- Application documentation
- Staff details form
- Superannuation documentation
- Competency Record
- Trainer Matrix
- Tax file declaration

Information is held in either a locked filing cabinet or electronically on the organisations hard drive or student management system. Access to information is limited to personnel with the correct authorisation and is only available to staff for the purpose of collection. Security measures such as unique password requirements and restricted file access are used to maintain and protect students/clients and employee's privacy. Where staff leave the organisation their access to data is removed/deleted.

Where a prospective student completes an online enquiry or payment – information is held in BSIL's email system, secure cloud server or accounting system XERO and is only available to the client solution managers for follow-up or finance team for the purpose of reconciliation & issuance of receipt.

3.3 Use of information

Personal information is only for the purpose for its collection and by staff who require the information in order to complete the tasks associated with their role and function.

i. Student personal information is used to;

- Identify individuals enrolled in an BSI Learning program
- Process application and enrolment requests including credit transfer applications
- Process payments for service delivered
- Monitor student progression and provide individualised support
- Enter student assessment results
- Identify students enrolled in a training product that is superseded
- Report data required by government (data provision and contractual data requirements).
- Monitor and evaluate organisational performance.
- Ensure certification documentation is awarded to the correct graduate

ii. Staff personal information is used to;

- Ensure staff have the correct qualifications, registration/licensing requirements to deliver and assess nationally recognised training.
- To mitigate risk and ensure student safety
- To support human resources processes and systems
- Manage logistical requirements associated with training and assessment
- Meet superannuation and taxation legislative requirements

Where students do not wish to use their name and contact details on assessment task submission sheets they are able to use their student or enrolment number.

3.4 Direct Marketing

BSI Learning only uses or discloses personal information for direct marketing purposes if consent has been gained. Individuals have the opportunity to be removed from circulation or subscription lists if they choose not to receive organisation related materials.

3.5 Disclosure of personal information

BSI Learning only discloses information to a third party where written consent has been gained from the individual. Where possible, data is encrypted so that the student has a level of pseudonymity. BSI Learning does not disclose any individual's personal information to overseas recipients.

In accordance with legislative and regulatory requirements BSI Learning is regularly required to provide information to State and Commonwealth government departments for the purpose of administration, research and quality assurance[5]. BSI Learning does not use or disclose government related identifiers.

[5] AVETMISS data, quality indicator reporting data and information required to undertake a compliance audit.

3.6 Accessing and seeking correction of personal information

BSI Learning acknowledges the rights of individuals to have access to their personal information under the "Freedom of Information Act' and provides opportunities to review this information on request.

Students and staff are encouraged to update their personal information as it changes to maintain the currency and accuracy of records/data. Where BSI Learning staff identify/suspect that personal information is inaccurate, out of date, incomplete or misleading they will contact the individual for further clarification and action any rectifications as required. Student is requested to send in writing via email or a letter the updated personal information. Student records in the student management system are then updated to reflect the new details. There is no charge to an individual who wishes to correct personal information or an associating statement.

3.7 Destruction of personal information

Personal information is stored in the organisations electronically (student management system) for a minimum period of 30 years. Hard copy documentation is securely destroyed in accordance with the organisations '*Records Management Policy and Procedure'*. See this policy and procedure for more information.

3.8 Complaints and appeals

Feedback on the organisations compliance with the privacy policy and procedure is encouraged by contacting the consumer protection officer or by making a complaint. Details of the Consumer Protection Officer are provided below.

Consumer Protection
mailto: consumerprotection@bsilearning.com.au
T: 1300 137 504

A complainant or appellant is required to lodge the complaint/appeal in writing. The Consumer Protection Officer will acknowledge the complaint within 48 hours of the complaint being received. Following a comprehensive investigation potential causes of the complaint will be identified, corrective actions taken to eliminate or mitigate the likelihood of future reoccurrence. The complainant will be informed of the outcome of their complaint within 10 days of their complaint being received. If the complainant is dissatisfied with the outcome of their complaint they can escalate their complaint to the Chief Executive Officer or request an independent review of their case. Failing to resolve the complaint at this level the complainant can approach the OAIC for further information and/or action. See Complaints and appeals policy and procedure for more information.

3.9 Governance mechanisms

BSI Learning has robust governance framework in place to ensure its compliance with the Australian Privacy Principles. The following governance framework underpins and supports the operationalisation of this policy and procedure;

- Risk assessments including privacy impact assessments are undertaken when required.
- Staff receive training on the handling of personal and sensitive information on employment commencement and as changes and/ or amendments occur.
- Staff who regularly handle personal information are provided with supervision and support from their line manager.

- Performance development and management processes ensure staff have the knowledge and skills required to complete their role requirements
- Where an agent or contractor is collecting personal information from a consumer on behalf of BSI Learning systematic processes are implemented to monitor compliance and maintain the student's privacy– see Engagement and Monitoring of Third Party Provider's Policy and Procedure.
- The Privacy Policy and Procedure is publically available on the website and a synopsis can be found in the student's handbook.
- The organisations Privacy Policy and Procedure is reviewed and updated annually or where required. Where changes to the Privacy Policy and Procedure have occurred the latest document version will be placed on the website and all students/clients will be notified by SMS that a new privacy policy and procedure has been released.
- BSI Learning takes all reasonable steps required to protect and maintain personal and sensitive information in accordance with the Australian Privacy Principles. If a data breach was to occur the organisation has a systematic approach to managing the critical incident in an open and transparent manner that manages risk effectively. The process for managing a data breach includes conducting a preliminary assessment and investigation, undertaking a risk assessment, notifying all relevant parties and developing an action plan to prevent potential future breaches.
- The organisations Continuous Improvement Committee monitors the effectiveness of the policy/procedure and is actively involved in its review.

4. References

- Australian Skills Quality Authority (2015) *"Standards for Registered Training Organisations (RTOs) 2015"*.
- Privacy Act 1988
- Privacy Amendment Act 2012
- Office of the Australian Information Commissioner () Australian Privacy Principles
- Office of the Australian Information Commissioner (2014) Guide to developing an APP privacy policy