PRIVACY AND CONFIDENTIALITY

1. PURPOSE

ICG Training and Consultancy Services Pty Ltd (ICG) is committed to providing quality training and assessment products and services in accordance with the Standards for Registered Training Organisations (SRTOs 2015). This Policy ensures that ICG manages personal information in accordance with the National Privacy Principles.

ICG is committed to protecting the privacy of the personal information it collects and receives. This Privacy Policy seeks to explain how ICG collects, uses, discloses, and otherwise handles personal information. It also seeks to explain how clients can access and correct the personal information held by ICG or lodge a complaint regarding any suspected privacy breach. In this regard ICG abides by the Privacy Act 1988 (Commonwealth) and relevant state legislation.

2. SCOPE

This policy forms part of ICG 's Quality Management System and applies to all business operations.

3. POLICY STATEMENT

ICG only collects information that relates to a client's enrolment and takes all reasonable steps to protect personal information from misuse, loss, unauthorised access, modification or disclosure including restricted access to electronic files, secure storage of paper files and back up of data.

Information concerning clients made available to ICG through the provision of registration or enrolment forms will be used for the purposes of general student administration, general communication, provision of course information, state and national reporting, program monitoring and evaluation.

Information will be provided to all such government agencies and/or organisations so authorised to receive such information where the provision of this information is necessary for ICG to continue to operate as a registered training organisation and for registration and re-registration purposes.

ICG is required to interact with ASQA in order to maintain registration. This includes the provision of students' files which may be accessed by ASQA representatives. ICG is also required to collect and report 'Total VET Activity' data. This includes full Australian Vocational Education and Training Management Information Statistical Standard (AVETMISS) data, in accordance with the National VET Provider Collection Data Requirements Policy.

This data is provided to the National Centre for Vocational Education Research (NCVER), who is authorised to disclose information to the Australian Government Department of

Education, Skills and Employment (DESE), Commonwealth authorities, State and Territory authorities (other than registered training organisations) that deal with matters relating to VET and VET regulators for the purposes of those bodies.

ICG will not disclose information about students to a third party, such as an employer, without written permissions from the student.

4. PROCEDURES

4.1 Collecting Information

a) When a student enrols with ICG, they are required to provide a name and email address, home address, telephone number and payment information. In some instances, they may be required to provide their date of birth, concession number or various educational/personal details depending on the course in which they are enrolling.

b) Information held by ICG regarding a student could include:

i. Student name.
ii. Current & previous address.
iii. Telephone numbers.
iv. Email address.
v. Drivers licence number.
vi. Bank account details.
vii. Passport number.
viii. Assessment results.
ix. Counselling or intervention strategies.
x. Interim transcripts.
xi. File notes.

c) ICG may collect information from clients having visited ICG's website including, IP address, browser, computer's operating system, application version, language settings and pages accessed.

d) ICG will only collect personal information for purposes which directly relate to provided services, and only when necessary. These purposes include:

i. Enquiries regarding enrolment.
ii. Submission of assessment material.
iii. Accessing other service programs.
iv. Direct mailing requests.
v. Applying for employment.
vi. When consulting with stakeholders.
vii. Planning public relations events.
viii. Conducting industry consultations.
ix. Submitting a complaint.

e) ICG will also collect personal information during standard communication processes directly related to those purposes, including:

i. When an individual emails a staff member.
ii. When an individual phones ICG their contact number may be stored.
iii. When an individual provides a business card.

4.2 Using and Disclosing Information

a) ICG only use personal information for the purposes for which it was provided, or for purposes which are directly related to the provision of ICG services. Personal information is only provided to external government agencies, organisations, or authorities when:

i. The individual has given permission.
ii. The individual would reasonably expect, or has been told, that information of that kind is usually passed to those individuals, bodies or agencies.
iii. It is required or authorised by law.
iv. It will prevent or lessen a serious and imminent threat to somebody's life or health.

b) ICG may use personal information provided by students for communication with the student, including marketing of their services. ICG must always provide within the marketing communication an opt-out function to allow the recipient of the communication the option to no longer receive communication from ICG.

4.3 Data Quality

a) ICG holds personal information in a number of ways, including in electronic databases, email contact lists, and in paper files held in drawers and cabinets, locked where appropriate. ICG's policy is to take reasonable steps to:

i. Ensure that personal information collected, use and disclose is accurate, up to date, complete and (in the case of use and disclosure) relevant.
ii. Protect the personal information held from misuse, interference, and loss and from unauthorised access, modification or disclosure.

4.4 Data Security

a) Steps used by ICG to secure personal information include IT security (such as encryption, firewalls, anti-virus software and login and password protection), secure office access, personnel security and training and workplace policies.

b) ICG process enrolments through online technologies. All transactions processed will meet industry security standards to ensure payment details are protected.

c) ICG uses a third party Student Management System to store information. The developers does not have permission to access or use any information that is stored in the systems, unless specifically requested by ICG in writing.

4.5 Access and Correction

a) Students have a right to request access to personal information that ICG holds about them and to request its correction.

b) Students wishing to access their records, are required to contact ICG and are required to provide proof of evidence, which may include:

i. Photo identification – drivers licence, passport, proof of age card.
ii. Date of birth.
iii. Contact details they provided upon enrolment.

c) Where refusal of access to information is being given by ICG, notification of this decision must be provided within fourteen (14) days. The reason for refusal must be provided in writing and referral to the compliant policy procedure given.

d) Where ICG agree to provide access to personal information as requested, access to the information must occur within fourteen (14) days of request.

e) Students can request to have their personal information corrected as required, for example, when a student wishes to change their maiden name to their married name. Evidence of the change may be requested by ICG before the correction is made.

f) No fees are charged for requests to access information or requests for correction of information.

4.6 Retention

a) All personal data that has been collected will only be kept for a limited duration that is relevant to the purpose for which the personal data is to be used and for as long as required by applicable law.

4.7 Breaches

a) The Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act 1988 (Privacy Act) established requirements for entities in responding to data breaches. ICG recognises that it has data breach notification obligations when

a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

b) The NDB scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'.

c) If ICG suspect an eligible data breach has occurred, reasonable and expeditious assessment will be undertaken to determine if the data breach is likely to result in serious harm to any individual affected.

d) When ICG is aware of reasonable grounds to believe an eligible data breach has occurred, individuals at likely risk of serious harm will be promptly notified. The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach.

e) The notification to affected individuals and to the Office of Australia Information Commissioner must include the following information:

   i. The identity and contact details of the organisation.
   ii. A description of the data breach.
   iii. The kinds of information concerned.
   iv. Recommendations about the steps individuals should take in response to the data breach.

f) The notification to the Commissioner can be made using the OAIC's Notifiable Data Breach form.

5. VARIATIONS

ICG reserves the right to vary, replace or terminate this policy from time to time.

6. DEFINITIONS

As defined in the Quality Management Strategy.

7. RELATED DOCUMENTS

- Student Enrolment Policy Procedure.
- Management of Records Policy Procedure.
- Code of Conduct.