

# Privacy Protection Policy

SOLUTION TO  
GROW YOUR  
GREATEST  
ASSETS - YOUR  
PEOPLE

[www.ipsinstitute.com](http://www.ipsinstitute.com)

5/38-40 Mill Street  
Yarrabilba  
QLD  
4207



# IPS Institute Privacy Protection Policy

IPS Institute collects and stores personal and sensitive information on our students and industry clients. In doing this, IPS Institute has introduced this policy to comply with our obligations under the Privacy Act. Protecting personal and sensitive information is essential not only to comply with the Privacy Act but also to safeguard IPS Institute staff and students from potential financial or reputational harm. Mishandling personal and sensitive data can lead to breaches of trust, significant reputational damage, and potential loss of enrolments, business partners, and revenue. Additionally, losing or compromising personal and sensitive information that is crucial to our operations can severely impact our ability to deliver services effectively.

Implementing robust personal and sensitive information security practices offers tangible benefits, including streamlined and efficient processes within the IPS Institute operation. It substantially reduces the risk of privacy breaches and minimises the resources required to manage and resolve any incidents that may occur. Many of the strategies outlined in this policy will also enhance our ability to handle other sensitive information, such as confidential information, effectively and responsibly.

## 1. Authority to collect and store information

IPS Institute is an approved Registered Training Organisation by the National VET Regulator. This registration is issued under the authority of the National Vocational Education and Training Regulator Act 2011. This legislation requires IPS Institute to collect personal and sensitive information from our students. This requirement is specified in the *Data Provision Requirements 2020* which is one of the legislative instruments that IPS Institute must comply with as a condition of its registration.

The *Data Provision Requirements 2020* require IPS Institute to collect data from students in accordance with the Australian Vocational Education Training Information Statistical Standard (AVETMISS). This is a complex information standard that defines information about who the student is, where the training is delivered and what they are studying. The Compliance Standards for RTOs require IPS Institute to retain and store this information for



**up to 30 years** and to report training activity to government agencies in accordance with mandatory reporting requirements.

In addition to the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014* also requires IPS Institute to collect high risk personal information for the purpose of creating or verifying a student's Unique Student Identifier. Together, these requirements form a statutory obligation to collect, store and report information of any student participating in nationally recognised training with IPS Institute.

## **2. Use of personal information**

To comply with its obligations under the *Data Provision Requirements 2020*, the *Student Identifiers Act 2014*, or contractual obligations or to facilitate an outcome of a service offered to students, IPS Institute will use personal information to comply with reporting obligations to Government agencies at the Commonwealth level and if accessing Government subsidised training also with a relevant State or Territory Government agency. Under some circumstances such as to facilitate an outcome of a service (such as licencing), IPS Institute may also need to report personal information to other relevant Government or responsible agencies. Students enrolling into a course with IPS Institute are advised of our collection and use of personal information with the *Student Handbook* sections related to "Your Privacy" and "National VET Data Policy".

## **3. Solicited information**

Contact information such as name, organisation, position, address, telephone, and email are collected for marketing, support services, mandatory reporting and for communicating with stakeholders as part of our day-to-day operation.

In addition to the collection of training activity information, IPS Institute will also collect, store and report information relating to satisfaction surveys, complaint handling and on our client employers.

Names, addresses, phone numbers, emergency contact details, bank account details and other employment related information is collected from employees for the purpose of managing human resources. The management of staff personal information complies with this policy.

## **4. Sensitive information**

Personal information collected by IPS Institute that may be regarded as 'sensitive' under the Privacy Act includes:

- 'Disability' and 'long-term impairment status' (health); and 'indigenous status', 'language spoken at home', 'proficiency in spoken English', 'country of birth' (implies ethnic/racial origin). This information is specified in the AVETMISS data elements and is collected for the national VET data collections, national VET surveys, and may be collected for VET-related research.
- 'Dietary requirements' (health-related) are collected for event catering purposes only.
- Biographical information, which may contain information on 'affiliations' and 'membership of a professional or trade association' are obtained from keynote speakers for event marketing purposes.
- 'Memberships of professional associations' and 'health and work injury information' is collected from IPS Institute employees for HR management purposes.

#### **5. Direct marketing**

IPS Institute respects an individual's right not to receive marketing material and provides an option within communications and on its website for individuals to unsubscribe from receiving marketing material. IPS Institute conducts its marketing communications and dissemination of service information in accordance with Australian Privacy Principle 7 (Direct marketing), the Spam Act 2003 (in respect of electronic communications), and the Do Not Call Register Act 2006. It is not IPS Institute practice to 'cold call' for the purpose of marketing its products and services. IPS Institute is not to undertake in unsolicited marketing practices, ever.

#### **6. Unsolicited personal information**

Unsolicited personal information is information IPS Institute may receive without actively asking for it. If IPS Institute should receive unsolicited personal information, it will be treated and managed according to the APPs. This means IPS Institute will need to assess the information to determine if holding the information is lawful. This includes assessing if the information could have been collected if actively sought by IPS Institute in the first place in accordance with Australian Privacy Principle 3 (Collection of Solicited Personal Information) and, is it necessary for IPS Institute to hold the information to perform its function and service to students? If the answer to either of these questions is no, IPS Institute is to destroy or de-identify the information as soon as practicable and inform the owner of the information of the actions.

The following is a practical example of protecting unsolicited personal information: A parent of a student sends an email to IPS Institute with records of their young adult son's medical history and condition. IPS Institute did not request this information and does not require it



for any reasonable purpose in providing services to the student. In this scenario, the Office Manager with the CEO should promptly evaluate the information. This evaluation would determine that IPS Institute could not have lawfully collected private medical information, it must securely destroy or de-identify the information as soon as possible and advise the parent and student of this action.

#### **7. Notification of collection**

IPS Institute aims to notify individuals of the collection of their personal information before, or at the time of collection, or as quickly as possible thereafter. Notifications are usually in writing but may be verbal by phone. Examples of notification include:

- Marketing – notification is provided on our website course application page. Individuals are also notified at the time of collecting personal information for events. A privacy notice is provided in all IPS Institute marketing communications.
- Pre-enrolment information supplied to the prospective student prior to their enrolment or commencement includes the Student Handbook. Students enrolling into a course with IPS Institute are advised of our collection and use of personal information with the *Student Handbook* sections related to “*Your Privacy*” and “*National VET Data Policy*”.
- Quality Indicator surveys – notification is provided in the email of invitation to participate in the surveys and also at the time of collecting the information.
- IPS Institute staff – Notification is provided on employment commencement.

#### **8. Disclosure of personal information**

IPS Institute is not to disclose personal information other than for the purpose for which it was collected, or an individual has consented to a secondary purpose, or an individual would reasonably expect this (such as receiving communications about upcoming events), or if required by law.

IPS Institute may share personal information with the Commonwealth government in accordance with Commonwealth contractual or regulatory obligations. In these circumstances, IPS Institute will take reasonable steps to inform and seek consent from the individuals concerned and take all reasonable steps to ensure that the recipient handles the personal information according to the APPs.

IPS Institute is not to sell or distribute mailing lists or student contact information to third parties under any circumstance. IPS Institute does not disclose personal information to overseas recipients. While people around the world can access material published on our website, no publications on our website are to contain identifiable personal information.

#### **9. Management of personal information**

IPS Institute will ensure the personal information it collects and uses or discloses is accurate, up to date, complete and relevant. IPS Institute routinely updates the information held in its student management system. This includes confirming with students who are returning for a new enrolment if their personal contact details have changed.

#### **10. Access to and correction of personal information**

Individuals may, subject to the exceptions prescribed by the APPs, request access to and correction of their personal information where this is collected directly from individuals by IPS Institute.

IPS Institute does not charge for giving access to or for correcting personal information unless the student is requesting copies to be made of information which may incur an administrative fee. Requests for access to or correction of personal information should be made in accordance with the access to records arrangements outlined in the *student Handbook*.

#### **11. Retention and recording of high risk personal information**

In accordance with the *APPs principles 11.2* and *Student Identifiers Act 2014*, section 11, IPS Institute is not to continue to hold information where it has no further purpose for this information. An example of this may include high risk personal information (refer to definitions) which may include a copy of a student passport, drivers' licence or Medicare Card. Once the student's identification or eligibility has been verified (the purpose), IPS Institute is to destroy through shredding or permanently deleting these records so that these records are no longer being stored by IPS Institute. IPS Institute's information security risk is significantly reduced if these records are destroyed as soon as possible after the purpose for collecting this information has been satisfied.

IPS Institute is to retain the details of high risk personal information that is used for the purpose of verification by recording the type of information that was viewed, the date it was viewed and by who. This is an acceptable record for the purpose of meeting our compliance obligations and is an effective risk avoidance strategy that is to be applied. As an example, instead of collecting and storing the actual record the following is acceptable: