

# Privacy Policy Statement

Prestige Employment Solutions (PES) is strongly committed to maintaining the privacy of personal information it collects as part of the services it offers. We place great importance on protecting the privacy of our employees, valued participants, customers and other stakeholders.

## Purpose

The purpose of this policy is to:

- Give you a better and more complete understanding of the kinds of personal information that we collect and hold.
- Clearly and concisely communicate how and when your personal information is collected, disclosed, used, held and otherwise handled by us.
- Inform you about the purposes for which we collect, hold, use and disclose personal information.
- Provide you with information about how you may access your personal information, and seek correction of your personal information.
- Provide you with information about how you may make a complaint, and how we will deal with any such complaint.

## Policy Statement

This policy sets out how we will comply with our obligations under the *Privacy Act 1988* (Cth) (**Act**). We are bound by the Australian Privacy Principles (**APPs**), which regulate how we may collect, use, disclose and hold your personal information, and how you may access and correct personal information held about you.

We will ensure that all of our officers, employees and subcontractors are aware of and understand our obligations and their own obligations under the Act and are provided with training to enable them to fulfil these obligations.

We will also achieve this through maintaining internal policies and processes to prevent personal information being improperly collected, held, shared / exchanged, accessed or disposed of.

## **What is personal information?**

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. It includes your name, date of birth / age, gender and contact details as well as health information (which is also sensitive information). In this privacy policy, a reference to personal information includes sensitive / health information.

## **Collection of personal information**

We do not collect personal information unless it is reasonably necessary for, or directly related to, one or more of our functions or activities.

Personal information collected by us will usually fall into one of the following categories:

- Contact information (name, age, address, email address and telephone numbers);
- Commonwealth identifiers (e.g. CRN, TFN).
- Employment information (e.g. employment history, work performance, absences, workplace incidents, next of kin information).
- Financial information (e.g. bank account details).
- Sensitive information (e.g. health, medical history, criminal history, religious beliefs, trade union activity).
- Information obtained to assist in managing customer and business relationships.

We may collect your information from you in a variety of ways including face-to-face, over the telephone, through an on-line form or portal, through a paper form or by email. Sometimes we will collect personal information from a third party or a publicly available source if it is unreasonable or impracticable to collect the personal information directly from you (e.g. checking a candidate's work history).

You may choose to deal with us anonymously or under a pseudonym where lawful and practical. Where anonymity or the use of a pseudonym will render us unable to provide the relevant service or reasonably conduct business, we may request that you identify yourself. For example, it would not be practical to deal with you anonymously if we are providing assistance in securing paid employment for you or referring you to other appropriate supporting services.

Where personal information is sensitive information, we will only collect that information where:

- It is reasonably necessary for one or more of our functions,
- We have the individual's consent to the collection of that information, or
- We are required or authorised by law to collect the sensitive information.

## **Why do we collect, use and store your personal information?**

We collect, use and store your personal information to provide you with direct and referral services including:

- Recruitment / Employment Services
- Employee Management
- Work capacity Assessment
- Labour Market Research
- Occupational Safety and Health
- Psychological Assessments / Counselling
- Insurance Claims and Assessments
- Training / Education
- Research
- Services under the National Disability Insurance Scheme
- Customer and Business Relationship Management

We may also collect, use and store your personal information for marketing purposes in order to inform you of the services we offer.

Our services, functions and activities, as well as those of our contracted service providers, may change from time to time.

## **Protecting and storing your personal information**

We are committed to keeping personal information secure and safe. Some of the ways we do this are:

- Requiring employees and contractors to enter into confidentiality agreements
- Securing hard copy document storage (i.e. storing hard copy documents in locked filing cabinets)

- Security measures for access to computer systems to protect information from unauthorised access, modification or disclosure and loss, misuse and interference
- Password protected data storage devices such as laptops, tablets and smart phones
- Providing a discreet environment for confidential discussions
- Access control for our buildings including waiting room / reception protocols and measures for securing the premises when unattended
- Security measures for our website

PES reviews and updates these measures from time to time to ensure security is maintained.

Personal information may be stored in documentary form but will generally be stored electronically on our software or systems.

Although we take all reasonable steps to secure personal information from loss, misuse and unauthorised access, there is an inherent risk of loss of, misuse of or unauthorised access to such information. We will not be held responsible for such actions where the security of the personal information is not within our control or we cannot reasonably prevent such an incident, for example, a technical malfunction, computer virus, third party interference or any action or event that is beyond our reasonable control.

### **Who will we disclose your personal information to?**

We will only use and disclose personal information for the primary purpose for which it was initially collected, or for purposes which are directly related to one of our functions or activities.

Like many other businesses in Australia, we contract out some of our functions and rely on third party suppliers or contractors to provide specialised services such as third party IT system, "cloud computing" technology and data storage services, legal advice, insurance broking, security services, business advisors and financial services. If personal information is provided to these suppliers, advisors and contractors in order to enable them to perform the agreed tasks, we will take reasonable measures to ensure that the supplier, advisor or contractor handles the personal information in accordance with the Act and the APPs. For example, we require all suppliers, advisors and contractors to provide privacy undertakings and enter into confidentiality agreements where they may have access to personal information.

We will not disclose your personal information to government agencies, private sector organisations or any third parties unless one of the following applies:

- You have consented
- We believe that you would reasonably expect, or have been told, that information of that kind is usually passed to those individuals, bodies or agencies
- It is otherwise required or authorised by law
- It is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body (e.g. police, ASIC, Immigration Department)

### **Accuracy of Personal Information**

We will ensure that all personal information we collect, use or disclose is accurate, complete and up-to-date. Please contact PES' Management if you are aware of any personal information that does not meet this objective.

If we are aware that we hold personal information that (having regard to the purpose for which it was collected) is inaccurate, out of date, incomplete, or irrelevant, we will take reasonable steps to correct that information.

You may seek access to, and correction of, personal information held by us in accordance with the section below "How can I access my personal information and contact PES?"

### **Will my personal information be transferred overseas?**

PES will not transfer your personal information overseas.

### **How can I access my personal information and contact PES?**

You can request access to personal information that we hold about you.

The procedure for requesting and obtaining access is as follows:

- All requests for access to personal information to be made in writing and addressed to our Management Team (see contact details below). All requests should specify how the information is proposed to be accessed (photocopies, electronic copy, or visual sighting)
- Please provide as much detail as possible regarding the person to whom you believe your personal information has been provided and when. This will allow us to process your request more efficiently
- We will acknowledge your request within 14 days of the request being made
- Access will usually be granted within 14 days of our acknowledgment. If the request cannot be processed within that time for whatever reason, we will let you know the anticipated timeframe for a response to be provided

- You will need to verify your identity and authority before access to personal information is granted
- We may charge a reasonable fee for access to personal information, which will be notified and required to be paid prior to the release of any information. Once the request has been processed by us, you will be notified of our response and proposal for suitable access (provision of photocopies, digital copies or visual sighting, where appropriate).
- We may refuse to grant access to personal information under certain circumstances (see below).
- If, as a result of access being granted, you are aware that we hold personal information that you regard as being no longer accurate or incorrect, you may request the deletion or correction of such information.
- Upon receipt of a request to correct or delete personal information, we will either make such corrections or deletions or provide written reasons as to why we declined to make such alterations (see below).

Under the Act, we may refuse to grant access to personal information if:

- We believe that granting access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety
- Granting access would have an unreasonable impact upon the privacy of other individuals
- Denial of access is required or authorised by law or by a Court or Tribunal order
- Giving access would be unlawful
- The request for access is frivolous or vexatious
- Legal proceedings are underway or anticipated and the information would not be accessible by way of the discovery process in those proceedings
- Giving access would reveal the intentions of PES in relation to negotiations between PES and you in such a way as to prejudice those negotiations
- Giving access is likely to prejudice enforcement related activities conducted by, or on behalf of, an enforcement body
- Giving access is likely to prejudice action being taken or to be taken with respect to suspected unlawful activity or serious misconduct relating to our functions or activities
- Giving access would reveal information in connection with a commercially sensitive decision-making process.

If we do not agree to make a correction to personal information, you may provide a statement about the requested corrections, and we will ensure that the statement is

apparent to any users of the relevant personal information.

If we do not agree to provide access to personal information or to correct the personal information, we will provide you with written reasons for the refusal and the mechanisms available to complain about the refusal.

PES' CEO is responsible for the management of:

- Requests for access to personal information.
- Complaints regarding our management of personal information.
- Coordination of employee training.

[feedback@pesau.net.au](mailto:feedback@pesau.net.au)

## **How do we handle complaints?**

If you consider that there has been a breach of the Australian Privacy Principles, you are entitled to complain to PES.

All privacy related complaints are to be directed to the CEO using the contact details above. In most cases a Privacy Complaint Form will need to be completed. PES will acknowledge receipt of a written complaint.

PES' CEO will investigate the complaint and attempt to resolve it within 5 business days after the written complaint was received. Where it is anticipated that this timeframe is not achievable, we will contact the person making the complaint to provide an estimate of how long it will take to investigate and respond to it.

## **Monitoring and training**

Compliance with this Privacy Policy is subject to internal and regulatory audit. PES will comply with all reporting requirements of the Act as they exist from time to time.

All staff will receive training with regard to privacy and the application of this Privacy Policy as part of their induction.