



# WORKFORCE INTERNATIONAL GROUP

## Privacy Policy

---

### National Privacy Principles

The National Privacy Principles established by the Privacy Act 1988, as amended, apply to all Workforce International Group companies and associated entities.

We only seek to collect personal information that is necessary for the proper performance of our tasks and functions. So far as is practicable, we may decline to collect unsolicited personal information from or about you and may take such measures as we think appropriate to purge it from our systems.

### Type of Personal Information Held

Personal information that we collect and hold usually falls into the following categories:

- candidate information submitted and obtained from the candidate and other sources in connection with applications for work;
- work performance information;
- information about incidents in the workplace;
- staff information;
- information submitted and obtained in relation to absences from work due to leave, illness or other causes;
- information obtained to assist in managing client and business relationships.

### Purposes for which we Hold Personal Information

We primarily hold personal information for the following:

- placement operations;
- recruitment;
- staff management;
- training;
- client and business relationship management;
- marketing

### Disclosures

We may disclose your personal information for any of the purposes for which it is primarily held or for a related secondary purpose.

In some cases we may only disclose information with your consent.

We may disclose your personal information where we are under a legal duty to do so, including circumstances where we are under a lawful duty of care to disclose information.

### Personal Information Quality

We rely on you to tell us when there are changes to your personal information that we hold about you. Examples might be a change of address or employment status.



## **Personal Information Security**

We take reasonable steps to destroy or permanently de-identify personal information when it is no longer required for any purpose for which it may be used or disclosed. However, it is not always

practicable to destroy or de-identify electronic data. Where it is not reasonable to destroy or permanently de-identify personal information in electronic form, we will take reasonable steps to prevent inadvertent access to it.

## **Inquiries and Complaints**

You can make further inquiries or complaints about privacy issues to our Privacy Coordinator whose contact details are: National HR and Customer Relations Manager. Tel: (02) 9310 6900

You can also make complaints to the Office of the Federal Privacy Commissioner.

## **Trans-Border Data Flows**

We cannot guarantee that any overseas recipient of your personal information will protect it to the standard to which it would be protected in Australia. The costs and difficulties of enforcement of privacy rights in foreign jurisdictions and the impracticability of attempting to enforce such rights in some jurisdictions will, mean that in some instances, we will need to seek your consent to disclosure into a jurisdiction in place of seeking an assurance of protection from the overseas jurisdiction.

## **Access**

Subject to some exceptions that are set out in the National Privacy Principles, you can gain access to the personal information that we hold about you.

We do refuse access if it would interfere with the privacy rights of other persons or if it breaches any confidentiality that attaches to that information.

If you wish to obtain access to your personal information you should contact our Privacy Coordinator. You will need to be in a position to verify your identity. You should also anticipate that it may take a little time to process your application for access as there may be a need to retrieve information from storage and review information in order to determine what information may be provided.

Chief Executive Officer – 1<sup>st</sup> June 2017