

PRIVACY POLICY



WHERE THIS POLICY APPLIES

This policy applies to all Workpower businesses and services.



RELEVANT LEGISLATION

- ↓ Privacy Act 1988 (Cth)
- ↓ National Disability Insurance Scheme Act 2013 (Cth)



RELATED DOCUMENTS

- ↓ Australian Privacy Principles
- ↓ NDIS Practice Standards

POLICY SCOPE

Workpower respects the privacy of its employees, participants, members, suppliers, contractors, customers and volunteers.

Information is managed in accordance and compliance with the Commonwealth Privacy Act 1988 and the Australian Privacy Principles (APP's), alongside the NDIS Practice Standards. The APP's set standards for taking reasonable and practical steps to collect, store, use and disclose an individual's personal information and requires personal information held by organisations to be complete, accurate and secure. It also allows individuals to access their information. Organisations must take reasonable steps to ensure that personal information is protected from misuse, loss or unauthorised access or disclosure.

WHAT DOES THIS POLICY COVER?

Workpower's privacy policy covers the collection, storage, use, disclosure and security of personal details of our customers. We explain how and when we collect personal information, what that information is used for, who uses it and when it may be disclosed to other parties. The policy also explains how you can access your personal information.

APP 1 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

Personal information refers to 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (Privacy Act 1988). For the purposes of this Policy:

- Personal information refers to information that relates to individuals and which identifies them (e.g. an individual's name, address, telephone number or photograph).
- Personal information includes information obtained from an individual or a third party, and the details relating to an individual's credit worthiness and credit history.

APP2 ANONYMITY AND PSEUDONYMITY

Workpower gives individuals the option of not identifying themselves, or of using a pseudonym. Wherever it is lawful and practicable, Workpower will provide individuals with the option of not identifying themselves when engaging in any transactions.

APP 3 COLLECTION OF SOLICITED PERSONAL INFORMATION

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- some aspects of biometric information

There is a higher standard to the collection of sensitive information and consent is required to collect sensitive information. Workpower will only collect relevant personal and sensitive information through lawful and fair means, directly from individuals where possible, and advise them if personal or sensitive information has been collected or needs to be collected from another individual or organisation.

Workpower will obtain written consent for all personal information collected. Information may be collected from various sources including:

- Directly from individuals via forms;
- Families, carers or advocacy organisations;
- Government and Non-Government Organisations such as the Department of Social Services, National Disability Insurance Scheme, Centrelink, Department of Communities, Commonwealth Respite and Carelink Centres and others.

The personal information Workpower generally collects includes an individual's name, address, telephone number and email address. We also collect personal information from individuals accessing

Workpower's services and/or programs. The collection of personal information is necessary for Workpower to provide services and to maintain relationships.

APP 4 DEALING WITH UNSOLICITED PERSONAL INFORMATION

Unsolicited personal information is personal information received by an entity that has not been requested by that entity. If Workpower receives unsolicited personal information it will determine whether or not it could have collected the information under APP 3, and:

- if Workpower could not have collected the personal information and the information is not contained in a Commonwealth record — then Workpower must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so, or
- if Workpower could have collected the personal information under APP 3, or the information is contained in a Commonwealth record, or the entity is not required to destroy or de-identify the information under APP 4.3 because it would be unlawful or unreasonable to do so — then Workpower may keep the information but must deal with it in accordance with APPs 5–13.

APP 5 NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Sensitive information is only collected to enable Workpower to effectively provide its range of services after justifying the need and legality to collect and hold such information. Workpower only discloses sensitive information collected to third parties with prior consent or where required by law.

Where Workpower collects personal information about an individual, reasonable steps must be taken to either to notify the individual of certain matters or to ensure the individual is aware of those matters.

The matters include:

- Workpower's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- Workpower's usual disclosures of personal information of the kind collected by the Workpower
- Workpower APP Privacy Policy
- whether Workpower is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located

Workpower must take reasonable steps, before, or at the time it collects personal information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

APP 6 USE AND DISCLOSURE OF PERSONAL INFORMATION

When Workpower collects personal information, it may use that information only for a purpose related to Workpower's business. Workpower will not use personal information for any other purpose without the individual's prior consent, unless required by law.

Workpower may use personal details for purposes including: tailoring activities and programs to individuals; ensuring the health and safety of individuals; to comply with Government agency requirements; promoting events, or advising the person of other Workpower services.

Workpower will only disclose personal information to third parties with the prior consent of the individual or where required by law. Consent may be by power of attorney or by an authorised carer if the individual lacks the capacity to consent.

APP 7 DIRECT MARKETING

Workpower may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

Workpower does not transfer personal and sensitive information overseas.

APP 9 ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

Workpower does collect some identifiers, but does not adopt, use or disclose identifiers of an individual that has been assigned or contracted by the Commonwealth Government (e.g. a Tax File Number).

APP 10 QUALITY OF PERSONAL INFORMATION AND APP 13 CORRECTION OF PERSONAL INFORMATION

Workpower will take reasonable steps to ensure that personal and sensitive information collected, used or disclosed is accurate, complete and up to date. If an individual believes their personal and sensitive information held is inaccurate, incomplete or out of date, they can advise Workpower by contacting the Privacy Officer (see contact details below).

Workpower provides individuals with access to the personal and sensitive information held about them upon request. Individuals may request the correction of the personal and sensitive information held about them. There may be exceptions to this where:

- It relates to a serious threat or impact upon another individual's privacy;
- The request is considered frivolous or vexatious;
- It relates to legal proceedings;
- It is commercially sensitive information or may affect negotiations;
- Access is unlawful or denial of access is authorised by law; or
- Access would prejudice statutory or legal obligations.

All requests to access an individual's personal and sensitive information must be made in writing. The individual will be required to provide proof of identity (e.g. a passport or driver's licence) to validate their authenticity to ensure that private information is not being disclosed to unauthorised individuals.

Access will be provided within five working days.

APP 11 SECURITY OF PERSONAL INFORMATION AND APP 12 ACCESS TO PERSONAL INFORMATION

Workpower will take reasonable steps to protect personal and sensitive information held from misuse, loss or unauthorised access or disclosure.

Electronic information is stored at each location and is backed up to an offsite third-party information services provider. Personal and sensitive information is secured and access is assigned to specific log-in ID's on an as required basis after management approval. Some electronic information is stored on Government databases that have their own security protocols controlled by the relevant Government Department.

Paper and hard copy records are kept in locked cabinets accessible only by those with authorisation. Workpower will destroy or permanently de-identify all personal and sensitive information no longer needed (e.g. by placing documents in a confidential bin and wiping clean computer disks).

The Notifiable Data Breaches (NDB) scheme under Part IIIIC of the Privacy Act 1988 (Privacy Act) outlines the notification obligations related to data breaches. Workpower is required to report data breaches to the OAIC and affected individuals within certain timeframes where there is unauthorised access or disclosure of personal information that is likely to cause serious harm that cannot be prevented with remedial action.

COMPLAINTS

If you are dissatisfied with the way we have handled your personal information, we would like to hear from you. You can contact the Complaints Officer, who will follow up your complaint.

Workpower welcomes complaints and feedback on our services enables us to make improvements. We will endeavour to resolve all complaints internally and as quickly as possible. If we are unable to resolve the complaint satisfactorily, you can make a request to the Australian Information Commissioner to have your complaint investigated. For more information about how to lodge a complaint please visit the Office of the Australian Information Commissioner <https://www.oaic.gov.au/individuals/how-do-i-make-a-privacy-complaint>.

From December 1 2020, if we are unable to resolve your complaint you can make a request through the NDIS Quality & Safeguarding Commission to have your complaint investigated. For more information on how to lodge a complaint please visit the NDIS Q&S Commission [website: https://www.ndiscommission.gov.au/](https://www.ndiscommission.gov.au/)

CONTACT US

Email: complaints@workpower.asn.au

Phone: Shane O'Connor, Executive Manager Corporate Services, on 0417 186 552

Post: Complaints Officer

Workpower Incorporated

PO Box 1543

Osborne Park

WA 6916

END OF DOCUMENT