Privacy Policy

MBC Employment Services is committed to upholding the Australian Privacy Principles contained in the Privacy Act 1988 (Cth) and any relevant amendments. We recognise the importance of privacy and awareness regarding the collection, use, disclosure and security of personal and sensitive information which we may collect during the course of our many functions. This Privacy Policy sets out how we manage personal and sensitive information and protect privacy.

Introduction

MBC Employment Services will only collect personal and sensitive information that is necessary to delivery our services including Employment Services in accordance with the Employment Services DEED. The type of information we may collect and hold varies depending on the purpose for which it is collected:

Customers: as a recipient of, or participant in our services, we may need to collect private information including your name and contact details, information regarding your health, income status, and emergency contact details.

Employees: as an employee, we may need to collect information about your name and contact details, bank account and taxation details, qualifications, previous experience and emergency contact details.

Sensitive information will only be collected as required for the delivery of services and in accordance with the Employment Services DEED and Privacy Act.

Collection and safety of personal and sensitive information

How we collect and store personal and sensitive information varies depending on the purpose for which it is collected but may include the collection of:

- copies of written correspondence;
- copies of receipts and/or transaction records;
- copies of application forms, request for assistance and/or other associated documents and information that you may provide to us in relation to service delivery;
- copies of employment agreements and any associated documents.

We may keep copies of the above documents (in physical or electronic form) as is necessary to carry out our functions and provide our services. All personal and sensitive information is securely stored at all times by us or an authorised external service provider and only authorised people will have access to the above documents and information.

Collection and holding of personal and sensitive information

We may collect, hold, use and disclose personal and sensitive information for purposes necessary to carry out our functions and provide our services in accordance with the Privacy Act.

We are committed to maintaining privacy and we will only use personal and sensitive information for a permitted purpose for which we have collected the information.

Information Sharing

If necessary to carry out our functions and provide our services, we may need to disclose personal and sensitive information to external service providers in accordance with the Privacy Act.

We will only share your personal and sensitive information in accordance with your express consent and instructions, as provided through the exclusions set out in the Australian Privacy Principles.

Access to Personal information

Customers have the right to access their personal and sensitive information, subject to some exceptions allowed by law. For security reasons should customers wish to access their information, this request must be in writing to the MBC Operations Team.

To enable us to verify your request we require you to advise the following:

- Your full name
- Address
- Contact phone number

Privacy Complaints or Comments

We are committed to protecting privacy and upholding the Australian Privacy Principles. If a customer believes we have breached the Australian Privacy Principles please contact our Operations Team in accordance with the MBC Complaints Procedure. Where resolution is not met, customers may lodge a complaint with the Office of the Australian Information Commissioner.

We take all complaints very seriously and we will endeavour to respond to your complaint and address your concerns as soon as reasonably practicable.

Internal Privacy Procedures

Collection and Disclosure of private information – All private and and confidential information collected must be for the purposes of delivering services. Any information collected as part of the Employment Services contract will meet the requirements of the Privacy Act and it's Australian Privacy Principles (as listed at the end of this document). Disclosure of private and and confidential information must be for

the purposes of delivering the Employment Services contract and meet Employment Services DEED and Privacy Act requirements.

Clean Desk - All private and confidential information, whether it be on paper, a storage device, or a hardware device, must be properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

Whenever a desk is unoccupied for an extended period of time the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as DVDs, and USB drives.
2. All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins.
3. Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and fax machines should be treated with the same care under this policy:
    a. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the “Secure Print” functionality should be used.
    b. All paperwork left over at the end of the work day will be properly disposed of.

Office Access – Any person entering the MBC office space must be supervised at all times by an MBC staff member.

Passwords – All passwords used by MBC staff must meet the following requirements:

- a minimum length of 10 characters, consisting of at least three of the following character sets:
- lowercase alphabetic characters (a-z)
- uppercase alphabetic characters (A-Z)
- numeric characters (0-9)
- special characters

Record Storage and Management – all private information must be securely stored in accordance with the Privacy Act. Secure bins must be used to discard of private information at MBC sites. All private information must be destroyed securely in accordance with the Employment Services DEED and Privacy Act.

Non-Conformance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Privacy Act Principles – Summary

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

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

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.