

MCI Institute Privacy Policy

Privacy Policy Statement

This Privacy Policy applies to Management Consultancy International Pty Ltd trading as MCI Institute (MCI), a subsidiary of APM Human Services International Pty Ltd (APM).

MCI's collection, use, disclosure and storage of your personal information is regulated by the *Privacy Act 1988* (Cth), the Australian Privacy Principles and related legislation.

Updates to this Privacy Policy will be published on our website.

If you have any questions regarding this Policy or our privacy practices generally, please do not hesitate to contact our privacy officer (details below).

Purpose

The purpose of this Privacy Policy is to:

- Give you an understanding of the kinds of personal information that we collect and hold.
- 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.

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

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

- Contact information (name, date of birth, age, gender, contact details including postal address, email address, telephone numbers and / or mobile telephone numbers).
- Commonwealth identifiers (e.g. CRN, TFN).
- Unique Student Identifier (USI).
- Information obtained to assist in managing client and business relationships.
- Employment information (e.g. educational history, reasons for study, employment history, work performance, absences, workplace incidents, next of kin information).
- Financial information (e.g. bank account details).
- Sensitive information (e.g. information about your race or ethnicity, health, medical history, criminal history, religious beliefs, trade union activity).

We may collect your information from you in a variety of ways including when:

- we provide services to you;
- you visit our website or social media platforms;
- you submit your information in response to MCI marketing events or activities; or

- you contact us by any method, such as face-to-face, over the telephone, through an online 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, for example where we have your consent, where we are required by law to do so, or 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. However, in some circumstances, anonymity or the use of a pseudonym will render us unable to provide the relevant service or reasonably conduct our business, and we may request that you identify yourself. For example, it would not be practical to deal with you anonymously if we are interviewing you for employment with MCI.

You may also choose not to provide us with your personal information. Depending on the circumstances in which you do so, however, we may be unable to provide you with our services as a result.

Where we are collecting personal information from a child or young person, we will use our judgement to determine if that person has the capacity to consent. Where we are unsure, we will seek consent from a parent or guardian.

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

We collect, use and store your personal information to provide you with our services which include:

- Training / Education.
- Research and analysis.
- Client and Business Relationship Management.
- Facilitating course and seminar enrolments.
- Verifying your identity to allow you to access to our online systems.
- Assessing your entitlement to Commonwealth assistance.
- Confirming that your USI is correct.
- Providing information, products, and / or services that you request.
- Personalising your experiences on our websites.
- Providing support and product updates.

We may also collect, use and store your personal information:

- for marketing purposes, in order to provide you information about the services we offer;
- to respond to your questions or suggestions;
- to improve the quality of our services;
- to improve the quality of your visit to our website.
- to undertake employee recruitment activities; or
- to assist with data analytic processes.

You may opt out of receiving marketing information by notifying us accordingly, or by using any unsubscribe facility we provide for that purpose. If you opt out of receiving marketing information, we may still contact you in connection with the services we provide to you, such as for appointment reminders and follow-ups.

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 understand the importance of 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);

- Implementing security measures for access to computer systems to protect information from unauthorised access, modification or disclosure and loss, misuse and interference;
- Ensuring data storage devices such as laptops, tablets and smart phones are password protected;
- Providing discreet environments for confidential discussions;
- Implementing access control for our buildings including waiting room / reception protocols and measures for securing the premises when unattended; and
- Implementing security measures for our website(s).

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

We may also need to keep your information for a significant time. For example, we will keep:

- Student records, certificates, and statements of attainment, in electronic format, for 30 years; and
- Assessment records for at least six (6) months.

Subject to applicable laws and our internal policies, we normally destroy or de-identify your information when we no longer need it.

Who will we disclose your personal information to?

Like most businesses in Australia, we contract out some of our functions and rely on third party suppliers or contractors to help us conduct our business, for example to provide specialised services such as employment services, "cloud computing" technology and data storage services, data analytic and marketing services, legal advice, insurance broking, security services, business advisors and financial services. We may disclose personal information to these third parties in connection with their provision of goods or services to us.

We may also disclose your personal information to other related entities within our corporate group for our own business purposes.

We may also disclose your personal information to government agencies, private sector organisations or other entities where required or permitted by law, which may include the following circumstances:

- You have consented to such disclosure.
- 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, and it is being disclosed for a purpose related (or directly related, in the case of sensitive information) to the reason we collected the information.
- We are required or authorised to make such disclosure by law or the requirements of any professional bodies, including where we are required to do so in accordance with child safety obligations.
- A permitted general situation or permitted health situation (as these terms are defined in the Privacy Act) exists in relation to the disclosure.
- We believe it is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body (e.g. police, ASIC, Immigration Department).

The persons to whom we disclose personal information are normally located in Australia, although personal information related to our staff and for our marketing activities may be disclosed to recipients outside Australia, including to recipients located in countries where MCI has offices. We may also use data hosting and cloud based service providers whose operations are located overseas. In all instances where this occurs, we will act in accordance with the Privacy Act and this Privacy Policy.

Accuracy of Personal Information

We take steps to help ensure that all personal information we collect, use or disclose is accurate, complete and up to date. Please contact our Privacy Officer (details below) if you are aware that personal information that we hold about you does not meet this objective.

How can I access my personal information and contact MCI?

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 Privacy Officer (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 MCI business, department and / or 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 endeavour to acknowledge your request within 14 days of the request being made.
- Access will usually be granted within 30 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 if there is an exception to such disclosure which applies under relevant privacy legislation.
- 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 correct, 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.

We have a designated Privacy Officer who is responsible for the management of:

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

For information regarding privacy, our Privacy Officer can be contacted at:



MCI Privacy Officer

58 Ord Street

WEST PERTH WA 6005



1300 768 550

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 MCI.

All complaints are to be in writing and directed to the Privacy Officer using the contact details above. In most cases, a Privacy Complaint Form will need to be completed. The Privacy Officer will endeavour to acknowledge receipt of a written complaint within 2 business days.

The Privacy Officer will investigate the complaint and attempt to resolve it within 20 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.

If you are unsatisfied with the outcome of MCI's investigation and decision, you are entitled to raise your complaint with the Office of the Australian Information Commissioner (OAIC) by phoning 1300 363 992 or by email at enquiries@oaic.gov.au.