Privacy Policy

MBC Accredited Training ('MBC') understands the importance people place on their privacy and personal information. As such we take privacy very seriously and comply with the requirements of the Australian Privacy Principles of the Commonwealth Privacy Act where they apply to our dealings with individuals. A copy of the Australian Privacy Principles can be accessed here. Where an inconsistency exists between this policy and the Australian Privacy Principles the Australian Privacy Principles will apply to the extent of any such inconsistency.

1.0 MBC will take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to our functions and activities that will ensure that we comply with the Australian Privacy Principles and that will enable us to deal with enquiries or complaints from individuals about our compliance with the Australian Privacy Principles.

1.1 MBC is required to collect Australian Government AVETMISS information about individual enrolments and report this information to State and Federal Government Departments on an ongoing basis. More detailed information on AVETMISS information can be found here. This information is collected in enrolment forms and stored in our student management system and reported to State Government reporting authorities each month and to the Federal Government at least once a year.

1.2 MBC also collects contact and communication information from the people that we deal from time to time (such as email address, name, home or work address, telephone and mobile numbers, diary notes of conversations with our staff etc). This information is collected from business cards, email signatures, direct discussions with people and from other communication sources and stored in our customer relationship management system for the purpose of maintaining accurate contact information and accurate records of communications.

1.3 MBC also collects anonymous demographic information, about our customers, such as their postcode, age, gender, preferences, interests and favourites in order to improve our segmentation of markets that we service.

1.4 MBC also collects analytical data about computer hardware and software that is used to access our website. This information can include: the user's IP address, cookie information, the pages you request, browser type, domain names, access times and referring Web site addresses. This information is used by MBC for the operation of our online services, to maintain and improve the quality of those services, and to provide general statistics regarding the use of those services.

1.5 MBC also stores personal information such as names, dates of birth and email addresses in our cloud based learner management system. Our learner management system is hosted by a US third party and all of the data is encrypted using SSL encryption. The Data Centers are located in the United States of America and each server is protected by biometric locks and round the clock interior and exterior surveillance monitoring.

1.6 MBC also stores personal information such as names, dates of birth, bank account details, email addresses and ledger account balance details in our accounting systems for the purpose of maintaining accurate account information for our debtor and creditor clients.

1.7 Unless advised in writing to the contrary Candidates permit MBC to publish any still photographic images and/or video/sound recordings taken of them and personal information such as their name, job role position, name of the organization they work for and it's location, the course that they are or were enrolled in and other information related to MBC's programs, activities and initiatives that they are or were involved in, on MBC's website blog and RSS feed and other related social media

sites that MBC's blog feeds into and that MBC uses, in newsletters uploaded to the web, in printed promotional material, in advertising, in displays and in competitions and local media. Workplace supervisors and employers/host employers also permit MBC to publish any still photographic images and/or video/sound recordings taken of them and/or their organisation and personal information such as the workplace supervisor's name, job role position, name of the employer's/host employer's organization and location, and other information related to MBC's programs, activities and initiatives that they are or were involved with, on MBC's website blog and RSS feed and other related social media sites that MBC's blog feeds into and that MBC uses, in newsletters uploaded to the web, in printed promotional material, in advertising, in displays and in competitions and local media. MBC also uses RSS Blog feeds and social media sites such as Facebook, Twitter, You Tube, Vimeo and Linkedin and any personally identifiable information or personally sensitive data disclosed directly by users on RSS blog feeds and public message boards on these sites may be collected and used by others. MBC will remove all published content covered by this consent from its sites and the social media pages and advertising mediums that it owns and controls if a candidate, workplace supervisor, employer or host employer later decides to withdraw this consent however MBC has no control over information that is or has been shared or broadcasted by other people or organisations.

1.8 MBC websites may contain links to other sites that are not under our control. These websites have their own policies regarding privacy. You should review those policies before visiting the websites. We have no responsibility for linked websites, and we provide these links solely for the convenience and information of our visitors.

1.9 MBC enforces a clean desk policy. Hard copy documentation such as enrolment forms that contain personal information are kept stored in locked cabinets or rooms and computers are password protected and put to sleep when operators are away from their desk. MBC operators

entering personal information into our software do so in circumstances where no one else is able to view the data being entered. All hard copy information is shredded and destroyed once electronic copies have been made.

2.0 Electronic information is backed up offshore using the Mozy Pro Secure Online Backup Service. This service is protected by Mozy Pro's military grade security that has successfully completed a SOC 1 SSAE 16 Type II audit and received ISO 27001 certification. MBC staff share documents in the cloud using the Drop Box service. Drop Box uses modern encryption methods to transfer and store data including Secure Sockets Layer (SSL) and AES-256 bit encryption and a two-step verification process. Both Mozy Pro and Drop Box data Centers are located in the United States of America.

2.1 Our student management system is hosted through the cloud via a contracted Australian third party. Student Management information is accessed by HTTPS 128 or 256 bit Secure Sockets Layer (SSL) with forms-based authentication. User login information is stored in encrypted LDAP databases and authentication is performed on every page request.

2.2 MBC ensures that third parties providing cloud-based services to MBC follow privacy protection at least equal to MBC's.

2.3 MBC will ensure that the information provided to us remains private and is used only for the purposes our customers agree to. We may reveal customer names and details of sales (product description and amount of sale) that have been made to our affiliates who have participated in our lead generation programs as this is how we calculate the lead generation and website advertising fees that are payable. MBC will not reveal, disclose, sell distribute, rent, license, share or pass personal information on to a third party without our customer's written consent.

2.4 In some cases we will be required by law (contractual and/or legislative

obligations) to make information available to others such as Registering Bodies from State or Federal Government Departments. MBC may also disclose your personal information in circumstances where you would reasonably expect us to do so, where it is reasonably necessary to lessen or prevent a serious and imminent threat to an individual's life or health or where it is reasonably necessary for the enforcement of criminal law. In all other cases we will ensure that we have the written permission of our clients.

2.5 Individuals may request access to and/or an update of their personal, enrolment and course outcome information by submitting a written request via email to MBC Admin. Upon substantiation of identity (and accuracy of the proposed amendments) records will be made available (and/or updated) within five (5) working days.

2.6 An individual's request to access or update their information can be dealt only with by authorised staff. Evidence of an individual's request is to be kept in their Student Management System file (eg. email from the individual, signed written request, diary note of the conversation etc).

2.7 A note must be made in their Student Management System file regarding how their identity was verified (eg. known personally by staff, showed drivers license number.. etc)

2.8 At times, Police may approach MBC for information regarding individuals. If Police want to interview an individual regarding law enforcement issues, staff are to pass on to Police the individual's whereabouts and other contact details. If Police want to inspect an individual's file and other documentation, they should be asked to provide the necessary legal documents to obtain such access. In both of the above cases Police should be asked to put their requests in writing. If information or access is given, a note detailing the circumstances must be made on the file. MBC's Director should also be contacted should assistance or advice be required.

2.9 MBC may receive requests from third parties requesting personal information about individuals. First, before any such information is released, a signed authorization from the relevant individual must be obtained. Secondly, if the signed authorization is not delivered in person by the individual, staff are to confirm with the individual that the authorization was not obtained under duress. Steps to obtain such confirmation would depend on the circumstances. A phone call may be in order if the private phone number is known and the staff member recognises the individual's voice. All formal requests for access to information about individuals are to be reported to the Director, including routine cases, for monitoring purposes and evidence of the formal request and authorization is to be kept in the individual's Student Management System file.

3.0 It is a term and condition of enrolment that all Candidates provide us with their irrevocable consent for confirmation and verification of certificates that have been issued to them to be provided to third parties upon presentation to MBC of the candidate's name, date of birth and the name of the course that the candidate purportedly completed.

3.1 It is a term and condition of enrolment that all Candidates provide us with their irrevocable consent for details regarding their course progress and academic conduct to be provided to employers and/or other stakeholders who have paid for, either in full or in part, their training and/or assessment.

3.2 It is also a term and condition of enrolment that all Candidates provide us with their irrevocable consent for details of any academic misconduct that they have been found guilty of to be published to third parties.

3.3 Individuals can complain about a breach of the Australian Privacy principles by following the procedures outlined in MBC's Complaint's Policy (or Staff Grievance Policy where applicable).