

Privacy Policy of RMIT Training Pty Ltd

1. *Policy Statement*

RMIT Training Pty Ltd ("RMIT Training") is committed to protecting the privacy of any information volunteered by visitors to its websites, and staff, students, and others who have rights to log into them. RMIT Training complies with State of Victoria and Commonwealth of Australia privacy legislation through this RMIT Training Privacy Policy.

All users of RMIT Training's websites and services should ensure that they read and understand this Policy prior to using such websites or services. If you do not agree with this Privacy Policy, please do not use any RMIT Training website.

2. *Purposes*

The purposes of this Policy are to:

- establish guidelines for the responsible collection and handling of personal information by RMIT Training;
- inform individuals of their right to access information about them which is held by RMIT Training and to correct any errors in that information; and
- establish a complaints procedure for investigation and rectification of breaches of this Policy.

3. *Scope and Responsibility*

This Policy applies to personal information collected by RMIT Training concerning staff, students, prospective students, individual clients and other individuals. It does not apply to information about corporations.

This Policy must be observed by all RMIT Training staff, consultants, external contractors and students who have access to personal information held by RMIT Training.

4. *Privacy Principles*

The Privacy Act 1988 and Privacy Amendment (Private Sector) Act 2000 of the Commonwealth of Australia set out Privacy Principles which must be observed by organisations such as RMIT Training that collect and hold personal information. RMIT Training's rights and obligations with respect to personal information are based on those Privacy Principles. The Privacy Principles are set out in the Appendix to this policy document. If an individual suspects that one or more of these Principles have been breached by RMIT Training, they should immediately contact the Privacy Officer and follow the complaints procedure below.

In brief, the Privacy Principles require the following obligations:

- RMIT Training will collect personal information only if it is necessary for RMIT Training's functions or activities.
- RMIT Training will inform you of the purposes for which we collect personal information and will use personal information only for the purposes for which it is collected.
- RMIT Training will always explain what is being collected and how and by whom it is to be collected.
- RMIT Training will take all reasonable steps to protect personal information it holds about you from unauthorised access, modification or disclosure and will not use or disclose personal information about you except in the limited circumstances set out in the Privacy Principles.
- RMIT Training will use its best endeavours to ensure that personal information we collect, use or disclose is accurate and up-to-date.

5. Privacy Officer

RMIT Training shall appoint a Privacy Officer who will be responsible for the administration of this Policy. Specifically the Privacy Officer will:

- keep the records which are required to be kept under this Policy;
- investigate complaints concerning a breach of the Privacy Principles;
- inform and assist staff with respect to privacy issues.

In accordance with the this Privacy Policy, Ian Penney has been appointed as the Privacy Officer. He may be contacted for further information and advice on telephone 9925 8190 or by email privacy.training@rmit.edu.au

6. Complaints Procedure

The following procedure will apply if an individual considers that RMIT Training has breached a Privacy Principle in respect of that individual:

1. A written complaint must be forwarded to the Privacy Officer within three (3) months of the time the complainant first became aware of the apparent breach. The complaint must specify details of the apparent breach.
2. The Privacy Officer must make a determination on the complaint within forty-five (45) days of receipt of the complaint, and advise the complainant in writing.
3. If the Privacy Officer determines that there has been a breach of the Privacy Principles, he or she will, upon notification of the determination to the complainant, advise relevant RMIT Training personnel in writing of any action required in order to remedy the breach. If the breach is capable of being rectified and is not rectified within thirty (30) days of the advice from the Privacy Officer, the Privacy Officer must inform the RMIT Training CEO.
4. The Privacy Officer will keep a record of complaints, and they will be tabled at meetings of the RMIT Training Executive Management Group.

7. Consequences if this Policy is Breached

Disciplinary action may be taken against any person who breaches this policy, including summary dismissal in the event of what RMIT Training considers to be a serious breach by a staff member.

Appendix

Privacy Principles

1. Principle 1 – Collection

- 1.1 RMIT Training:
 - will collect personal information only if the information is necessary for one or more of its functions or activities;
 - must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.2 When RMIT Training collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of RMIT Training and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected (“the primary purposes”); and
 - (d) to whom (or the types of individuals or organisations to which) RMIT Training usually discloses information of that kind; and
 - (e) any law that requires the particular information to be collected; and
 - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.3 If it is reasonable and practicable to do so, RMIT Training will collect personal information about an individual only from that individual.

However, there will be instances where RMIT Training will obtain such information from other sources, e.g. references for employment purposes; results data for prospective students, verification of formal qualifications of staff and students etc. In such instances RMIT Training will take reasonable steps to ensure that the individual is or has been made aware of the matters listed in Principle 1.2 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Principle 2 – Use and Disclosure

RMIT Training will not without the prior consent of an individual use or disclose personal information about that individual for a purpose (the secondary purpose) other than the primary purposes of collection except in any of the following situations:

- (a) both of the following apply:
 - the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information¹, directly related to the primary purpose of collection;
 - the individual would reasonably expect RMIT Training to use or disclose the information for the secondary purpose; or
- (b) if the use or disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual:
 - it is impracticable for RMIT Training to seek the individual’s consent before the use or disclosure; and
 - in the case of disclosure – RMIT Training reasonably believes that the recipient of the information will not disclose the information; or
- (c) RMIT Training reasonably believes that the use or disclosure is necessary to lessen or prevent either:
 - a serious and imminent threat to an individual’s life, health, safety or welfare; or
 - a serious threat to public health, public safety or public welfare; or
- (d) RMIT Training has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (e) the use or disclosure is required or authorised by or under law; or
- (f) RMIT Training reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of a law enforcement agency:
 - the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction;
 - the enforcement of laws relating to the confiscation of the proceeds of crime;

¹ “Sensitive information” means information or an opinion about an individual’s racial or ethnic origin or political opinions or membership of political organisations or religious beliefs or affiliations or membership of trade or professional organisation or sexual preferences or practices or criminal record that is also personal information.

- the protection of the public revenue;
 - the prevention, detection, investigation or remedying of seriously improper conduct;
 - the preparation for, or conduct of, proceedings before any court or tribunal, or
- (g) the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Service (ASIS), in connection with its function, has requested RMIT Training to disclose the personal information and:
- the disclosure is made to an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) to receive the disclosure; and
 - an officer or employee of ASIO or ASIS (as the case requires) authorised in writing by the Director-General of ASIO or ASIS (as the case requires) for the purposes of this paragraph has certified that the disclosure would be connected with the performance by ASIO or ASIS (as the case requires) of its functions.

Any such disclosure under this paragraphs 2 (c) to 2 (g) inclusive can only be made by the RMIT Training CEO or Solicitor, and written note to that effect must be made.

3. Principle 3 – Data Quality

RMIT Training will take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up to date.

If RMIT Training is to ensure the quality and accuracy of personal information, this places an obligation upon an individual to provide relevant and accurate information to RMIT Training.

4. Principle 4 – Data Security

- 4.1 RMIT Training will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 4.2 RMIT Training will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

5. Principle 5 – Openness

- 5.1 RMIT Training will make this Policy available to anyone who asks for it.
- 5.2 On request by a person to the Privacy Officer, RMIT Training will take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Principle 6 – Access and Correction

- 6.1 If RMIT Training holds personal information about an individual, it will provide the individual with access to the information on request by the individual, except to the extent that:
- (a) providing access would pose a serious and imminent threat to the life or health of any individual; or
 - (b) providing access would have an unreasonable impact on the privacy of other individuals; or
 - (c) the request for access is frivolous or vexatious; or
 - (d) the information relates to existing legal proceedings between RMIT Training and the individual, and the information would not be accessible by the process of discovery or subpoena in those proceedings; or
 - (e) providing access would reveal the intentions of RMIT Training in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
 - (f) providing access would be unlawful; or
 - (g) denying access is required or authorised by or under law; or
 - (h) providing access would be likely to prejudice an investigation of possible unlawful activity; or
 - (i) providing access would be likely to prejudice:
 - the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction; or
 - the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - the protection of public revenue; or
 - the prevention, detection, investigation or remedying of seriously improper conduct; or
 - the preparation for or conduct of, proceedings before any court or tribunal, or implementation of its orders by or on behalf of a law enforcement agency; or
 - (j) ASIO, ASIS or a law enforcement agency performing a lawful security function asks RMIT Training not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

- 6.2 Where providing access would reveal evaluative information generated within RMIT Training in connection with a commercially sensitive decision-making process, RMIT Training may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
- 6.3 If RMIT Training is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (j) inclusive, RMIT Training will, if reasonable, upon request by the individual to RMIT Training's Privacy Officer consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.
- 6.4 RMIT Training reserves the right to charge for providing access to personal information, and if it does so it will:
 - (a) advise an individual who requests access to personal information that RMIT Training will provide access on the payment of the prescribed fee; and
 - (b) may refuse access to the personal information until the fee is paid.
- 6.5 If RMIT Training holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up to date, RMIT Training will take reasonable steps to correct the information so that it is accurate, complete and up to date.
- 6.6 If RMIT Training and the organisation disagree about whether the information is accurate, complete and up to date, and the individual asks the organisation to associate with the information a statement from the individual claiming that the information is not accurate, complete or up to date, RMIT Training will take reasonable steps to do so.
- 6.7 RMIT Training will provide reasons for denial of access or a refusal to correct personal information.
- 6.8 If an individual requests access to, or the correction of, personal information held by RMIT Training, RMIT Training will:
 - (a) provide access, or reasons for the denial of access; or
 - (b) correct the personal information, or provide reasons for the refusal to correct the personal information; or
 - (c) provide reasons for the delay in responding to the request for access to or for the correction of personal information as soon as practicable, but no later than forty-five (45) days after receiving the request.
- 6.10 RMIT Training is not required to provide an individual with access to information about that individual if that information is generally available to the public.

7. Principle 7 – Unique Identifiers²

- 7.1 RMIT Training will not assign unique identifiers to individuals (except for a Staff Number to identify a staff member, a Student Number to identify a student and a database primary key to ensure the uniqueness of a database record) unless it is necessary for RMIT Training to carry out its functions efficiently. Staff Numbers, Student Numbers and database primary keys are considered necessary for RMIT Training to carry out its functions efficiently.
- 7.2 RMIT Training will not knowingly adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation (except for staff & student numbers assigned by RMIT University).
- 7.3 RMIT Training will not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

8. Principle 8 – Anonymity

Because of the nature of some of RMIT Training's core businesses, it may be impractical for individuals transacting with RMIT Training to have the option of not identifying themselves. However where it is lawful and practical to do so, RMIT Training will give individuals this option.

9. Principle 9 – Transborder Data Flows

- 9.1 RMIT Training will only transfer personal information about an individual to someone (other than RMIT Training or the individual) who is outside Victoria if:
 - (a) RMIT Training reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the Privacy Principles set out in this Policy; or
 - (b) the individual consents to the transfer; or

² "Unique Identifier" means an identifier assigned by an organisation to an individual uniquely to identify that individual for the purposes of operations of the organisation but does not include an identifier that consists only of the individual's name.

- (c) the transfer is necessary for the performance of a contract between the individual and RMIT Training, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between RMIT Training and a third party; or
- (e) all of the following apply:
 - the transfer is for the benefit of the individual;
 - it is impracticable to obtain the consent of the individual to that transfer;
 - if it were practicable to obtain that consent, the individual would be likely to give it; or
- (f) RMIT Training has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Privacy Principles set out in this Policy.

10. Principle 10 – Sensitive Information

10.1 RMIT Training will not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required under law; or
- (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - is physically or legally incapable of giving consent to the collection; or
 - physically cannot communicate consent to the collection; or
- (d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite paragraph 10.1, RMIT Training may collect sensitive information about an individual if:

- (a) the collection:
 - is necessary for research, or the compilation or analysis of statistics, relevant to government funded targeted welfare or educational services; or
 - is of information relating to an individual's racial or ethnic origin and is collected for the purpose of providing government funded targeted welfare or educational services; and
 - there is no reasonably practicable alternative to collecting the information for that purpose; and
 - it is impracticable for RMIT Training to seek the individual's consent to the collection.