

PRIVACY POLICY

Massage and Beauty Education Pty Ltd

Trading as ACBT – Australian College of Beauty Therapy and ACMM – Australasian College of Massage & Myotherapy

RTO Code 53004 | ABN 61 676 503 594

Field	Detail	Field	Detail
Document ID	POL-014	Version	1.0
Approved by	Chief Executive Officer	Approval date	27 Oct 2026
Effective date	27 Oct 2026	Next review	review annually

This Policy is a controlled document. The current version is published on our website.

Website enquiry form – how we handle your information

When you submit an enquiry through our website, Massage and Beauty Education Pty Ltd (RTO Code 53004), trading as ACBT and ACMM, collects the details you enter – such as your name, email address, phone number, the course you are interested in and your message.

We use this information to respond to your enquiry and to send you the course information you ask for. If you do not give us your contact details, we cannot reply to you. We may tell you about our courses where you would reasonably expect it, and every message we send includes a simple way to unsubscribe.

Your enquiry is received by our RTO Office. It may also be accessed by our management in Japan and is stored with our email and cloud service providers in Japan, the United States and other countries (see section 10). We do not sell your information.

You can make a general enquiry without giving your full name (section 15). To access or correct your information, or to make a complaint, see sections 16 and 17 or contact us at admin@acbtmm.com.

1. Purpose and scope

1.1 Massage and Beauty Education Pty Ltd (we, us, our), trading as ACBT – Australian College of Beauty Therapy and ACMM – Australasian College of Massage & Myotherapy, is a Registered Training Organisation (RTO Code 53004). We collect and hold personal information about students, prospective students, clients of our student clinic, staff, trainers, assessors, contractors, work placement hosts and other individuals in the ordinary course of delivering nationally recognised vocational education and training.

1.2 The purpose of this Policy is to explain, in an open and transparent way, how we manage personal information, as required by Australian Privacy Principle (APP) 1 of the Privacy Act 1988 (Cth), and to give effect to clause 20 of the Standards for RTOs 2025 – Compliance Requirements,

which requires us to collect, use and disclose personal information in accordance with all applicable privacy laws and the Student Identifiers Act 2014 (Cth).

1.3 This Policy applies to:

- all personal information we collect, hold, use and disclose, in any format (paper, electronic, image, audio or video);
- all of our staff, trainers, assessors, contractors, volunteers and governing persons; and
- all of our training sites, our student clinic and our online learning environment, including personal information that is accessed or stored outside Australia (see section 10).

1.4 This Policy does not apply to the practices of external organisations to which we lawfully disclose personal information (for example, the National Centre for Vocational Education Research). Those organisations have their own privacy policies.

2. Our legal obligations

2.1 Privacy Act 1988 (Cth)

We comply with the Privacy Act 1988 (Cth) (Privacy Act) and the 13 Australian Privacy Principles set out in Schedule 1 to that Act.

2.2 Why the Privacy Act applies to us

Section 6D of the Privacy Act exempts certain small business operators with an annual turnover of \$3 million or less. That exemption does not apply to us, for the following reasons:

- (1) we provide a health service and hold health information. Our student clinic delivers remedial massage services to members of the public, and we collect client health histories, treatment records and student health declarations. An organisation that provides a health service and holds health information is not a small business operator (s 6D(4)(b)), regardless of turnover;
- (2) we may from time to time be a contracted service provider under a Commonwealth or State contract; and
- (3) in any event, our governing persons have resolved that we will comply with the Privacy Act and the APPs in full and will not rely on the small business exemption. This resolution is recorded in [governance meeting minutes reference].

Accordingly, the whole of this Policy is binding on us and on every person who handles personal information on our behalf.

2.3 Other requirements that govern our handling of personal information

Instrument	What it requires of us
Standards for RTOs 2025 – Compliance Requirements	Clause 20: comply with all applicable privacy laws and the Student Identifiers Act 2014. Clause 10: retain certification records for 30 years and assessment records for 2 years after completion, and give students access to their certification records. Clause 12: verify each USI and never print a USI on a qualification or statement of attainment. Clause 17: written agreements with any third party that delivers services on our behalf.
Standards for RTOs 2025 – Outcome Standards	Standard 2.1: clear, accurate and accessible information for students before enrolment. Standard 2.7: an accessible complaints system. Standard 4.2: roles and responsibilities of staff and third parties are documented. Standard 4.3: risks, including conflicts of interest, are identified and managed. Standard 4.4(2)(c): data is collected and analysed lawfully.

Instrument	What it requires of us
Student Identifiers Act 2014 (Cth)	Governs the collection, verification, use, disclosure and destruction of a Unique Student Identifier (USI). Unauthorised use or disclosure is an offence.
National Vocational Education and Training Regulator Act 2011 (Cth) and Data Provision Requirements 2020	Requires us to collect specified personal information about students, report it to the National VET Data Collection held by NCVER, and provide information to ASQA on request.
Spam Act 2003 (Cth); Do Not Call Register Act 2006 (Cth)	Govern electronic marketing messages and marketing telephone calls.
Fair Work Act 2009 (Cth) and Fair Work Regulations 2009	Require employee records to be made and kept for 7 years.
Work Health and Safety Act 2020 (WA) and Regulations	Require incident and health monitoring records to be made and retained.
Corporations Act 2001 (Cth) s 286	Requires financial records to be retained for 7 years.
Privacy and Responsible Information Sharing Act 2024 (WA)	Applies to Western Australian public sector bodies rather than to us directly. Where we act as a contracted service provider to a WA public sector body, we comply with the privacy obligations imposed by that contract.

We are not registered on CRICOS and do not enrol student visa holders. If this changes, this Policy will be amended to address the Education Services for Overseas Students Act 2000 (Cth) and the National Code.

3. Definitions

Term	Meaning
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.
Sensitive information	A subset of personal information with stronger protection, including health information, racial or ethnic origin (including Aboriginal and Torres Strait Islander status), membership of a professional or trade association, criminal record, religious beliefs, sexual orientation and biometric information.
Health information	Information about an individual's health or disability, a health service provided or to be provided to them, and personal information collected in the course of providing a health service.
USI	The Unique Student Identifier assigned to an individual under the Student Identifiers Act 2014 (Cth).
Overseas recipient	A person or organisation outside Australia, other than us or the individual concerned, to whom we disclose personal information.
Related company	TRTA Co., Ltd., a company incorporated in Japan that is related to us through common ownership.
Eligible data breach	Unauthorised access to, unauthorised disclosure of, or loss of personal information, that is likely to result in serious harm to one or more individuals.
Privacy Officer	The staff member appointed under section 24 with day-to-day responsibility for this Policy.

4. The personal information we collect and hold

4.1 We only collect personal information that is reasonably necessary for one or more of our functions or activities (APP 3). The kinds of information we collect are set out below.

4.2 Prospective students and applicants

- name, date of birth, gender, address, telephone and email;
- citizenship, residency or visa status, and passport details where required to confirm eligibility to study and to work in a clinical setting;
- previous education, qualifications, transcripts and evidence for credit transfer or recognition of prior learning;
- language, literacy, numeracy and digital literacy assessment results, and English language evidence where applicable;
- information about disability, medical conditions or other circumstances relevant to identifying the support and reasonable adjustments a student may need.

4.3 Enrolled students

- Unique Student Identifier (USI) and USI verification records;
- the AVETMISS data set required by the Data Provision Requirements 2020, which includes sensitive information: Aboriginal and Torres Strait Islander status, disability status, country of birth, main language spoken at home, and highest school level completed;
- enrolment, attendance, participation and progress records;
- completed assessment evidence, including written work, observation and third-party reports, and photographs, audio or video recordings of practical and clinical assessment;
- health declarations, immunisation status where required for clinical practice, and injury and incident records;
- national police certificate or working with children check where required for a placement or clinical activity;
- fee, payment, refund and debt records (we do not store full credit card numbers);
- emergency contact details;
- complaints, appeals, misconduct, welfare and support records;
- certification records – qualifications and statements of attainment issued.

4.4 Student clinic clients

- name, contact details, date of birth and emergency contact;
- health history, presenting complaint, medications, contraindications and informed consent to treatment;
- treatment notes and outcomes recorded by the student under supervision, and the supervisor's notes;
- appointment, payment and incident records.

Client records created in the student clinic are health records. They are subject to the additional controls in sections 8 and 13.

4.5 Staff, trainers, assessors and contractors

- identity and contact details, tax file number, superannuation and bank details;
- qualifications, training and assessment credentials, vocational competency evidence, professional development records and industry currency evidence;
- professional association membership, registration and insurance details;

- working rights evidence, police clearances and references;
- performance, validation participation, conduct and training records.

4.6 Other individuals

- work placement supervisors and host employer contacts;
- industry consultation participants;
- complainants, witnesses and other parties to a complaint or appeal;
- website visitors – see section 19.

5. How we collect personal information

5.1 Wherever it is reasonable and practicable to do so, we collect personal information directly from the individual concerned (APP 3.6), for example through enquiry forms, applications, enrolment forms, pre-training reviews, clinic intake forms, assessment activities, surveys and correspondence.

5.2 We may also collect personal information from third parties, including:

- a previous registered training organisation, school or university, for credit transfer or recognition of prior learning;
- the Student Identifiers Registrar, when we verify or apply for a USI with the individual's consent;
- the Department of Home Affairs VEVO service, when we verify visa and work entitlements;
- an employer, work placement host or supervisor, in relation to workplace-based assessment;
- a referee nominated by a job applicant;
- a parent or guardian, where the student is under 18; and
- government departments and funding bodies administering a subsidy for which the student has applied.

5.3 Unsolicited personal information. If we receive personal information we did not solicit, we will decide within a reasonable period whether we could have collected it under APP 3. If we could not, we will destroy or de-identify it as soon as practicable, if it is lawful and reasonable to do so (APP 4).

5.4 We do not adopt a government related identifier (for example a Medicare number or driver licence number) as our own identifier of an individual, and we do not use or disclose such identifiers except as permitted by APP 9. The USI is dealt with in section 7.4.

6. Notice at the time of collection

6.1 At or before the time we collect personal information (or as soon as practicable afterwards), we take reasonable steps to notify the individual of the matters in APP 5.2, including who we are, why we are collecting the information, the consequences of not providing it, the organisations to which we usually disclose it, that this Policy explains how to seek access and correction and how to complain, and whether we are likely to disclose the information overseas and, if so, to which countries.

6.2 We do this by giving the individual the applicable notice:

Individual	Notice given
VET student / applicant	Collection Notice and Student Declaration at Appendix A, incorporated into the enrolment form, together with the current NCVER Privacy Notice and the Department of Employment and Workplace Relations VET Privacy Notice.
Student clinic client	Client Privacy and Consent Notice at Appendix B, given at intake before any treatment.

Individual	Notice given
Staff, trainer, assessor, contractor	Employment or contractor privacy notice issued with the offer or engagement documentation.
Website visitor	This Policy and the website notice described in section 19.

6.3 We retain evidence that the individual has acknowledged the applicable notice – a signed or electronically acknowledged declaration – on the individual's file, and produce it to the VET Regulator on request.

7. Why we collect, hold, use and disclose personal information

7.1 We use and disclose personal information for the primary purpose for which it was collected, for a related secondary purpose that the individual would reasonably expect (directly related, in the case of sensitive information), where the individual has consented, or where the use or disclosure is required or authorised by or under an Australian law or a court or tribunal order (APP 6).

7.2 Our purposes include:

- assessing applications, conducting pre-training reviews and determining whether a training product is suitable for the applicant;
- enrolling students, delivering training and conducting assessment;
- identifying and providing training support, wellbeing support and reasonable adjustment;
- managing the student clinic, including client safety, informed consent and continuity of treatment;
- issuing, verifying and re-issuing qualifications and statements of attainment;
- meeting our reporting, record keeping and cooperation obligations as an RTO;
- administering fees, payments, refunds and debt recovery;
- managing complaints, appeals, misconduct and disciplinary matters;
- quality assurance, assessment validation, self-assurance and continuous improvement;
- work health and safety, incident investigation and insurance;
- recruiting, engaging and managing staff, trainers, assessors and contractors;
- communicating with students and, with consent, marketing our courses; and
- any other purpose required or authorised by Australian law.

7.3 Sensitive information

We collect sensitive information only where the individual consents and the information is reasonably necessary for one of our functions, or where the collection is required or authorised by law (APP 3.3). The AVETMISS data items listed in section 4.3 are collected because we are required by law to do so; students are told this in the Collection Notice.

7.4 Unique Student Identifier

The USI is subject to the Student Identifiers Act 2014 (Cth) in addition to the Privacy Act. We:

- apply for a USI on a student's behalf only with the student's consent;
- ask the Student Identifiers Registrar to verify each USI before we use it for any purpose (Compliance Requirements cl 12(1)(b));
- never include a USI on a qualification or statement of attainment (Compliance Requirements cl 12(1)(a)) or on any public-facing document;
- use and disclose a USI only for the purposes authorised by that Act;
- do not use the USI as our own internal student identifier;

- restrict access to USIs to staff who require it to perform their duties; and
- treat unauthorised use or disclosure of a USI as a serious disciplinary matter and as an incident under section 18.

8. Health information and the student clinic

8.1 Health information is sensitive information and attracts the highest level of protection under this Policy.

8.2 Before a client receives treatment in the student clinic we obtain written informed consent to:

- the collection of a health history and the creation of treatment records;
- treatment being performed by a student under the supervision of a qualified supervisor;
- the supervisor and, where relevant, other students in the supervised session having access to the client record for teaching and assessment purposes; and
- the use of de-identified case information for assessment, validation and teaching.

8.3 Case studies, reflective journals and assessment tasks submitted by students must be de-identified. A client's name, date of birth, address, contact details, images or any other identifying particulars must not appear in an assessment submission. Assessors must return a submission that identifies a client.

8.4 We do not disclose a client's health information to a third party (including the client's doctor, employer or insurer) without the client's written consent, unless the disclosure is required or authorised by law, or is necessary to lessen or prevent a serious threat to the life, health or safety of any individual.

8.5 Student health declarations are collected to manage safety in practical and clinical training. They are held separately from academic records and are accessible only to the Privacy Officer, the staff member responsible for student support and the trainer responsible for the activity.

9. Who we disclose personal information to

9.1 We disclose personal information to the recipients set out below. We do not sell personal information, and we do not disclose personal information for a third party's own marketing purposes.

Recipient	What is disclosed and why	Basis
Australian Skills Quality Authority (ASQA)	Student, assessment, trainer and governance records, for regulatory audit, investigation and registration.	Required by law (NVETR Act; Standards for RTOs 2025)
National Centre for Vocational Education Research (NCVER)	AVETMISS enrolment and training activity data for the National VET Data Collection, which may be used for statistical, regulatory and research purposes and for student surveys.	Required by law (NVETR Act; Data Provision Requirements 2020)
Student Identifiers Registrar	Identity details to create or verify a USI, and training outcomes linked to the USI transcript.	Student Identifiers Act 2014
Department of Employment and Workplace Relations; WA Department of Training and Workforce Development	Student and training activity data for policy, funding administration and audit.	Required or authorised by law / funding contract

Recipient	What is disclosed and why	Basis
Software and cloud service providers	Hosting and processing of records on our behalf under written terms (see section 10 for providers located outside Australia).	Necessary for our functions
TRTA Co., Ltd. (our related company in Japan)	Records needed to provide administrative, financial and IT support services to us.	Necessary for our functions; see section 10
Work placement hosts and supervisors	Student identity, unit requirements, insurance, clearances and assessment records for supervised placement.	Consent / necessary for delivery
Professional associations and health funds	Confirmation of qualification and course details, where the student asks us to support an application for membership or provider recognition.	Consent
Insurers, brokers, auditors, lawyers and consultants	Information necessary to obtain insurance, manage a claim, obtain advice or conduct an audit.	Necessary for our functions
Debt collection agents	Identity, contact and debt details where a fee remains unpaid after our internal process is exhausted.	Necessary for our functions
Parents, guardians or a nominated emergency contact	Limited information necessary in an emergency, or in relation to a student under 18.	Consent / serious threat
Police, courts, tribunals and other authorities	Information required by warrant, subpoena, notice or other legal process.	Required or authorised by law

9.2 We may also use or disclose personal information where we reasonably believe it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety, or where another permitted general situation or permitted health situation under the Privacy Act applies. Any such use or disclosure is recorded in the Privacy Incident and Disclosure Register, with the reason and the decision maker.

10. Personal information accessed or disclosed outside Australia

10.1 Access by our own management from Japan

Our Chief Executive Officer is based in Japan and accesses our records remotely in order to govern and manage the organisation. This is a use of personal information by us, not a disclosure to another organisation. This Policy, our security controls in section 12 and our accountability under the Privacy Act apply to that access in full.

10.2 Overseas recipients

We are likely to disclose personal information to the following recipients located outside Australia:

Country	Recipient	Purpose and information involved
Japan	TRTA Co., Ltd. (our related company)	Administrative, financial and IT support services provided to us under a written services and data handling agreement. Named personnel have role-based access to the records they need for those services.
Japan	GMO Pepabo, Inc. (Lolipop! email hosting)	Hosting of our organisational email accounts, which may contain personal information in correspondence.

Country	Recipient	Purpose and information involved
United States and other countries in which Google operates data centres	Google LLC (Google Workspace, including Gmail, Google Drive and Google Classroom)	Email, file storage, collaboration and our learning management system.
Australia and, for support and service operations, other countries	Microsoft (Microsoft 365)	Email, document and collaboration services.
New Zealand	Xero Limited	Accounting and payroll records.

Where a provider only stores or processes information on our behalf and we retain effective control of it, the arrangement may be a use rather than a disclosure under the Privacy Act. We list those providers and their locations in any event, so that individuals know where their information may be held.

10.3 Reasonable steps

Before disclosing personal information to an overseas recipient we take such steps as are reasonable in the circumstances to ensure the recipient does not breach the APPs (APP 8.1). Those steps include:

- written contractual terms requiring the recipient to handle the information consistently with the APPs and this Policy, to use it only for the purpose for which it was provided, to maintain security controls, and to notify us immediately of any suspected data breach;
- restricting overseas access to the minimum personnel who need it, using individually named accounts and multi-factor authentication;
- assessing each provider's security certifications and data storage locations before engagement, and reviewing that assessment at least annually through our Information Asset Register;
- requiring personnel of TRTA Co., Ltd. to complete our privacy training and sign a confidentiality undertaking before access is granted; and
- recording our arrangement with TRTA Co., Ltd. as a related-party arrangement in our conflicts of interest register, consistent with Outcome Standard 4.3.

10.4 Under section 16C of the Privacy Act we remain accountable for personal information we disclose overseas. An act done by an overseas recipient that would breach the APPs is treated as a breach by us.

10.5 We do not rely on the APP 8.2(a) exception (that the recipient is subject to a substantially similar law) unless we have obtained written advice to that effect for a specific disclosure. Where we rely on an individual's consent under APP 8.2(b), we will first inform the individual expressly that, if they consent, we will not be required to take reasonable steps to ensure the overseas recipient complies with the APPs.

10.6 TRTA Co., Ltd. handles personal information it receives from us in a manner consistent with this Policy and with the Act on the Protection of Personal Information (Japan), and has confirmed this to us in writing.

10.7 Services delivered on our behalf

TRTA Co., Ltd. does not recruit, market to, enrol or induct students, collect fees, deliver training or assessment, or issue certification on our behalf. If we engage any person, in Australia or overseas, to deliver services on our behalf within the meaning of the Standards for RTOs 2025 – Compliance

Requirements, we will, before the services commence, enter into a written agreement that meets clause 17, notify ASQA within the required timeframe, inform students of the arrangement (Outcome Standard 2.1) and update this Policy.

11. Direct marketing

11.1 We may use personal information to tell individuals about our courses, workshops, clinic services and events, where the individual would reasonably expect us to do so and we provide a simple means of opting out (APP 7).

11.2 We do not use or disclose sensitive information for direct marketing without the individual's consent.

11.3 Every commercial electronic message we send identifies us, includes our contact details and contains a functional unsubscribe facility, as required by the Spam Act 2003 (Cth). Unsubscribe requests are actioned within 5 business days.

11.4 An individual may ask us at any time not to use or disclose their personal information for direct marketing, and may ask us for the source of the information. We will comply within a reasonable period and at no charge.

11.5 Marketing consent is never a condition of enrolment, and withdrawing it has no effect on a student's training or assessment.

12. Quality and security of personal information

12.1 Quality

We take reasonable steps to ensure the personal information we collect, use and disclose is accurate, up to date, complete and relevant (APP 10). We ask students to confirm their details at enrolment, we verify identity documents and USIs, and we correct records promptly when advised of a change. Data quality checks are run before each AVETMISS submission.

12.2 Security

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11.1). Our controls include:

Control area	Measures
Access control	Individually named accounts; role-based permissions; multi-factor authentication on all accounts holding personal information; access reviewed on engagement, role change and exit; access removed on the last day of engagement. Shared or generic accounts are not used to access student records.
Technical	Encryption in transit and at rest; managed anti-malware; patching; automated backups with periodic restore testing; no storage of personal information on personal devices or personal cloud accounts.
Physical	Student and clinic files held in locked cabinets; clean desk and screen-lock rules; secure destruction; restricted access to the clinic records area.
People	Confidentiality clauses in every employment and contractor agreement; privacy induction before access is granted; annual refresher training; training records retained.
Vendors	Written terms with every provider that stores or processes personal information for us, covering purpose limitation, security, sub-contracting, breach notification and return or destruction of data on termination.
Email and transfer	Assessment evidence and health information transferred only through approved systems; sensitive files shared by permissioned link rather than attachment; recipient verified before sending.

12.3 The Privacy Officer maintains an Information Asset Register identifying, for each system holding personal information, what it holds, who has access, where it is hosted and who the provider is. The register is reviewed at least annually.

13. Retention and destruction

13.1 We retain personal information only for as long as it is needed for a purpose set out in this Policy, or for as long as we are required to retain it by law. Minimum retention periods are:

Record	Minimum period	Source / note
Records of AQF certification documentation issued (qualifications and statements of attainment)	30 years	Compliance Requirements cl 10(b). Students, including former students, can obtain copies (cl 10(d)).
Assessments submitted by students	2 years after the student completes the training product	Compliance Requirements cl 10(c). We retain completed assessment evidence for [3] years to support validation and appeals.
Enrolment and AVETMISS records	[7 years]	Data Provision Requirements and any funding contract conditions.
Student clinic client health records	7 years from the last service; for a client who was under 18, until they turn 25	No WA statute sets a minimum period for private providers. This period reflects accepted professional practice, limitation periods and insurer requirements.
Employee records	7 years from the end of employment	Fair Work Regulations 2009
WHS incident and health monitoring records	5 years (longer for specified hazards)	Work Health and Safety Act 2020 (WA) and Regulations
Financial records	7 years	Corporations Act 2001 (Cth) s 286
Complaints, appeals and investigations	[7 years] from closure	Continuous improvement and limitation periods.
Unsuccessful job and course applications	[12 months]	Then destroyed, unless the applicant asks us to retain them.

13.2 Where we no longer need personal information for any purpose for which it may be used or disclosed, and we are not required by law or a court or tribunal order to retain it, we destroy it or de-identify it (APP 11.2). Paper is destroyed by cross-cut shredding or a secure destruction service; electronic records are securely deleted from all systems and backups. Destruction is recorded in the Records Destruction Register.

13.3 If we cease to be registered as an RTO, we will comply with any direction from ASQA concerning student records and will make arrangements so that students can continue to obtain copies of their certification documentation.

13.4 Records subject to a current or reasonably anticipated legal proceeding, regulatory investigation or insurance claim are placed on legal hold and must not be destroyed, even if the retention period has expired. A legal hold is issued in writing by the Chief Executive Officer and recorded in the Records Destruction Register.

14. Automated decision-making

14.1 From 10 December 2026, APP 1 requires a privacy policy to state where a computer program uses personal information to make, or to do a thing substantially and directly related to making, a decision that could reasonably be expected to significantly affect an individual's rights or interests. Our current position is:

System / process	Position
Competency decisions	All competency judgements are made by a qualified assessor exercising professional judgement. Automated marking is not used.
Admission and pre-training review	Suitability, support needs and enrolment decisions are made by a person. [Insert any scoring tool used, or "manual".]
Learning and student management systems	Automated rules may generate reminders and progress alerts. Any decision affecting a student's enrolment, results or fees is made by a person.
Recruitment of staff	Applications are screened by a person.
Artificial intelligence tools	Personal information of students, clients or staff must not be entered into an AI tool unless the tool has been approved in writing by the Privacy Officer and is covered by terms meeting section 12.2. [Approved tools: none / list.]

14.2 We review this section whenever a new system is introduced and at least annually.

15. Anonymity and pseudonymity

15.1 An individual may deal with us anonymously or by pseudonym where it is lawful and practicable (APP 2), for example when making a general course enquiry, providing anonymous feedback or completing an anonymous survey.

15.2 It is not practicable to deal with a person anonymously for enrolment, assessment, certification, clinic treatment or employment, because we are required by law to identify the individual, obtain a USI and report identified data.

16. Access to and correction of personal information

16.1 Access (APP 12)

An individual may request access to the personal information we hold about them by contacting the Privacy Officer (section 27) and providing proof of identity. We will:

- acknowledge the request within 5 business days;
- respond within 30 calendar days;
- provide access in the manner requested where reasonable and practicable; and
- not charge for making the request. We may charge a reasonable, non-excessive fee for the cost of giving access, and we will tell the individual the amount beforehand.

If we refuse access, in whole or in part, we will give written reasons and the ground of refusal under APP 12.3, and explain how to complain. Where giving direct access to health information would pose a serious threat to the life, health or safety of any individual, we may give access through a mutually agreed health practitioner. Students may access their own assessment records and results; assessment tools, marking guides and model answers are not released where release would compromise assessment integrity.

16.2 Correction (APP 13)

We will correct personal information that is inaccurate, out of date, incomplete, irrelevant or misleading, on request or on our own initiative, within 30 calendar days and free of charge. If we have disclosed the information, we will notify the recipient on request unless it is impracticable or unlawful – this includes data reported to NCVER. If we refuse to correct, we will give written reasons and, on request, associate a statement with the record that the individual considers it inaccurate.

A request to change an assessment outcome is not a correction request. It is dealt with under our Complaints and Appeals Policy and Procedure.

17. Privacy complaints

17.1 An individual who believes we have breached the APPs or this Policy may complain to the Privacy Officer (section 27), in writing or verbally. We will help an individual who needs assistance to make a complaint, including in a language other than English.

17.2 We will acknowledge the complaint within 5 business days and give a written outcome within 30 calendar days. If more time is needed we will explain why. The complaint is investigated by a person not involved in the matter, and all parties are afforded procedural fairness.

17.3 No individual is disadvantaged for making a complaint. A student's enrolment, progress or assessment is not affected by making a privacy complaint.

17.4 If the individual is not satisfied with our response, or we have not responded within 30 days, they may complain to the Office of the Australian Information Commissioner (OAIC):

Office of the Australian Information Commissioner | GPO Box 5288, Sydney NSW 2001 | 1300 363 992 | www.oaic.gov.au

17.5 Privacy complaints are recorded in our Complaints Register, reported to our governing persons and used to inform continuous improvement (Outcome Standard 2.7). Complaints about training, assessment, fees or conduct are handled under our Complaints and Appeals Policy and Procedure.

18. Data breach response

18.1 We are subject to the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act.

18.2 Any staff member, trainer or contractor who becomes aware of a suspected data breach – including a lost device or file, a misdirected email, an unauthorised disclosure of a USI or a clinic record, or a suspected system compromise – must report it to the Privacy Officer immediately and in any case within 24 hours.

18.3 On receiving a report, the Privacy Officer will:

- (1) contain the breach and take immediate steps to limit further access or disclosure;
- (2) assess, within 30 calendar days, whether the incident is an eligible data breach;
- (3) take remedial action, documenting the reasoning where remedial action removes the likelihood of serious harm;
- (4) where the breach is an eligible data breach, notify the OAIC and affected individuals as soon as practicable;
- (5) notify any other party required by contract or law, including the Student Identifiers Registrar where USIs are affected, our insurer, and the Australian Cyber Security Centre where appropriate; and
- (6) record the incident and decisions in the Data Breach Register and report to our governing persons.

18.4 The detailed process, contacts and templates are in our Data Breach Response Plan, which is tested at least annually.

19. Website, online platforms and recordings

19.1 Our website collects information submitted through enquiry and application forms, and technical information such as IP address, browser type, pages visited and time of visit. We use [Google Analytics / insert tool] for site analytics. Cookies may be used; you can disable cookies in your browser, although some features may not work.

19.2 Our website may link to third party sites. We are not responsible for the privacy practices of those sites.

19.3 Online classes and meetings may be recorded for learning, assessment or quality assurance. Participants are told before recording starts, and a participant who does not consent may ask for an alternative arrangement. Recordings used as assessment evidence are stored in an approved system and retained under section 13.

20. Photographs, video and audio

20.1 We may photograph or record students during practical and clinical training where the recording is required as assessment evidence. Consent is obtained at enrolment using the form at Appendix C, and use is limited to assessment, validation and regulatory audit.

20.2 Use of a student's image, voice, name or work for marketing, on our website or on social media requires separate, specific, written consent, which may be withdrawn at any time.

20.3 Consent to marketing use is never a condition of enrolment or of a successful assessment outcome, and refusal has no consequence for the student.

20.4 Students and staff must not photograph or record a clinic client or another student without that person's express consent, and must not post any such material on social media.

21. Staff, trainers, assessors and contractors

21.1 Acts and practices directly related to a current or former employment relationship and an employee record are exempt from the APPs under section 7B(3) of the Privacy Act. We apply the standards in this Policy to employee records in any event.

21.2 The exemption does not apply to job applicants, contractors or volunteers. Their personal information is handled in full accordance with the APPs and this Policy.

21.3 Trainer and assessor credential, currency and professional development records are disclosed to ASQA on request. Trainers and assessors are informed of this at engagement.

21.4 Every staff member, trainer, assessor, contractor and volunteer must sign a confidentiality undertaking and complete privacy induction before being given access to personal information, and must complete refresher training annually.

22. Work placements and third parties

22.1 Where a work placement host or any other organisation receives personal information from us, our written agreement requires it to comply with the Privacy Act and this Policy, to use the information only for the agreed purpose, to maintain security, to notify us of any suspected breach, and to return or destroy the information at the end of the arrangement.

22.2 A student is told before a placement what information will be given to the host, and why.

23. Students under 18 and individuals needing assistance

23.1 If we enrol a student under 18, we obtain the written consent of a parent or guardian to the collection, use and disclosure of the student's personal information, in addition to the student's own acknowledgement, and we manage that information consistently with the National Principles for Child Safe Organisations (Outcome Standard 4.3(2)(d)).

23.2 We assess an individual's capacity to consent case by case. Where an individual does not have capacity, we deal with a parent, guardian or authorised representative and record the authority on the file.

24. Roles and responsibilities

Role	Responsibility
Governing persons	Approve this Policy; oversee privacy risk through the risk register; receive reports on privacy complaints and data breaches.
Chief Executive Officer	Accountable for compliance with the Privacy Act; approves legal holds and notification of an eligible data breach.
Privacy Officer – [Name, position]	Day-to-day owner of this Policy; maintains the Information Asset Register, Data Breach Register, Privacy Incident and Disclosure Register and Records Destruction Register; handles access, correction and complaint requests; delivers privacy training; conducts the annual review.
Trainers, assessors and all staff	Comply with this Policy; collect only what is needed; keep records secure; report a suspected breach within 24 hours; de-identify client information in teaching and assessment materials.
Contractors, service providers and placement hosts	Comply with this Policy and their written agreement with us.

25. Related documents

- Data Breach Response Plan
- Records Management and Retention Policy and Procedure
- Complaints and Appeals Policy and Procedure
- Student Clinic Operations and Supervision Procedure
- Electronic Assessment Submission Procedure
- Conflicts of Interest Policy and Register
- IT Acceptable Use and Information Security Procedure
- Registers: Information Asset Register; Data Breach Register; Privacy Incident and Disclosure Register; Records Destruction Register; Complaints Register; Privacy Training Register

26. Review

This Policy is reviewed at least annually by the Privacy Officer and approved by the Chief Executive Officer. It is also reviewed whenever there is a change in the law, a change to our systems, service providers or delivery arrangements, a data breach, or a complaint that reveals a gap.

27. How to contact us

Contact	Privacy Officer, RTO Office
----------------	-----------------------------

Post	Level 1, 863 Hay Street, Perth WA 6000
Email	admin@acbtmm.com
Telephone	08 6325 8097 (+61 8 6325 8097)
Policy available at	https://www.australasiancollegeofmassageandmyotherapy.com.au/privacypolicy – and on request, free of charge, in a reasonable alternative format