MotionMate Training

Privacy Policy

Effective Date: 06 January 2026 – Next Review: January 2027

1. Purpose

MotionMate Training (MMT) is committed to protecting and upholding the privacy rights of all our clients, including private clients, National Disability Insurance Scheme (NDIS) participants, and children under 18 years of age. This Privacy Policy outlines how MMT collects, uses, discloses, and secures personal and health information in the course of providing our physiotherapy services. We adhere to the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)** in all aspects of handling personal information. Our goal is to manage personal information in an open and transparent way, ensuring confidentiality while delivering high-quality mobile and online physiotherapy services.

2. Scope

This policy applies to all personal information collected and processed by MotionMate Training in Western Australia and through our online services globally. It covers information of clients (adults and children), their parents/guardians or representatives, NDIS participants (self-managed and plan-managed), and any other individuals who engage with MMT's services. All MMT representatives (employees, contractors, and volunteers) are expected to comply with this policy when handling personal or sensitive information on behalf of MMT. This policy is made available on our website and by request, and it is intended for use in both web and print formats for easy reference by our clients and stakeholders.

3. Definitions

Personal Information: Information or an opinion about an identifiable individual. Common examples include name, date of birth, address, phone number, email, and other contact details. If an individual's identity can reasonably be ascertained from the information, it is considered personal information.

Sensitive Information: A subset of personal information that is given a higher level of protection under the Privacy Act. It includes information about an individual's health, disability, racial or ethnic origin, sexual orientation, religious beliefs, or criminal history. **Health information** (such as medical history, treatment notes, and health service records) is a type of sensitive information that MotionMate Training frequently needs to collect to provide physiotherapy services. MMT will not collect sensitive information (including health information) without the individual's consent unless an exception under the law applies. (for example, if required by law or necessary to prevent a serious threat to life or health).

Client: Any individual who uses or is assessed for MMT's physiotherapy services. This includes adult clients, children under 18 receiving services (with consent of a parent or guardian), and NDIS participants. For children, "client" may refer jointly to the child and their parent/guardian.

NDIS: National Disability Insurance Scheme, an Australian government program providing support to people with disabilities. MMT provides services to **self-managed** and **plan-managed** NDIS participants (where the participant or their plan manager pays for services). Throughout this policy, references to disclosures or use of information for "NDIS participants" include interactions with their plan managers or support coordinators as needed for service provision.

You/Your: In this policy, "you" or "your" refers to any individual whose personal information we handle – typically our clients or their representatives.

We/Us/Our: Refers to MotionMate Training (MMT) and its team of healthcare professionals and staff.

4. Policy Statement

MMT respects and values the privacy of all individuals we serve. We recognize that the personal and health information you entrust to us is private and sensitive, and we have a duty of care to protect that information. We collect personal and sensitive information only for purposes directly related to our services – primarily to deliver safe and effective physiotherapy care – and we will **not** use or disclose it for other purposes without your consent, unless required or permitted by law. We are committed to maintaining confidentiality, implementing appropriate security measures, and ensuring that all handling of personal data is done in accordance with applicable laws, including the Australian Privacy Principles. This commitment extends to all forms of information, whether it's collected in person, over the phone, through our website, via email, or through third-party platforms we use (such as Cliniko, Stripe, and Microsoft 365 OneDrive).

MMT also acknowledges the special considerations required when dealing with children's personal information and information of individuals with disabilities. We handle all personal data – especially health information and children's data – with the utmost care and security, treating it in line with legal requirements and best practices for privacy.

5. Collection of Personal and Health Information

5.1 What We Collect:

We only collect personal information that is reasonably necessary for our functions or activities as a physiotherapy service provider. The types of personal information we may collect include:

- **Identification and Contact Details:** Name, date of birth, address, phone number, email address, and emergency contact information (for example, a parent or next of kin).
- **Health Information:** Medical history, current conditions or injuries, treatment plans, doctor or specialist reports, medications, and other health-related details necessary for assessment and treatment. This may also include health insurance or Medicare details and NDIS plan information if applicable.
- **NDIS and Disability Support Information:** For clients who are NDIS participants, we may collect your NDIS participant number, plan goals, support coordinator or plan manager contact details, and relevant support documents to ensure services align with your plan.
- **Financial and Billing Information:** Payment details, such as billing address or invoice information. **Note:** For payments processed via **Stripe**, we do **not** store full credit card numbers on our own systems – payment information is handled securely by Stripe, though records of transactions and receipts are maintained.

- **Children's Information:** For clients under 18, we collect the child's personal and health information as needed for treatment, as well as contact details and consent from a parent or legal guardian. We may also record the guardian's details (name, relationship, contact information) and any relevant information about guardianship or custody (if applicable to the child's care).
- **Other Information:** Any additional information you choose to provide to us or which is necessary for specific services – for example, feedback, inquiry details, or information provided through our complaint process.

We treat all of the above categories (especially health and disability-related information) as sensitive and handle them with a high level of security and confidentiality. We will not collect personal information that we do not need. In particular, we **do not** collect government-issued identifiers (such as Medicare numbers or driver's license numbers) unless it is necessary for us to perform our services or required for identity verification – and we never use such identifiers as our own internal ID for you.

5.2 How We Collect Information:

MotionMate Training collects personal information by fair and lawful means. We typically collect information directly from you or your authorized representative (such as a parent, guardian, or support coordinator). The ways we collect information include:

- **Direct interactions:** When you contact us or use our services, for example:
    - Through phone calls or in-person conversations (e.g. during consultations, assessments, or booking inquiries).
    - Via email or online contact forms (including any intake or registration forms you fill out on our website or through our practice management system **Cliniko**).
    - During therapy sessions and assessments (where we may take notes on your condition, progress, and any advice given).
- **Online services:** If you book appointments or use telehealth services through our website or affiliated platforms, we collect information you enter (such as health details on intake forms or your contact and payment information for booking). Our online forms and bookings may be facilitated by third-party software (e.g. Cliniko for bookings/scheduling and records, Stripe for payments). These platforms will transmit your information to us.
- **Third-party referrals:** With your consent, we may receive personal or health information from third parties involved in your care or support. For example:
    - Referrals or reports from your **general practitioner (GP)**, medical specialists, or other allied health professionals.
    - Information from your **NDIS support coordinator or plan manager** (for instance, a support coordinator might share your NDIS plan goals or reports so we can tailor our services to your needs, or a plan manager might provide billing authorization details).
    - In the case of a child client, information from schools, pediatricians, or other caregivers, with parental consent.
- **Public or other sources:** Generally, we will not collect your personal information from publicly available sources or third parties without consent. In rare cases, if needed and allowed by law, we might verify or obtain additional details from publicly available records

(for example, to confirm contact details or if attempting to reach a next-of-kin in an emergency).

When we collect information from someone other than you (the client), we will, whenever practical, make sure you know about it. For example, if a doctor or family member provides us with information about you, we will note it in your records and ensure you have provided consent for us to obtain that information.

5.3 Children's Personal Information:

Collecting and using information about children requires additional care. If you are under 18, we will ordinarily seek consent from your parent or legal guardian before collecting your personal and health information or providing services. We ask that a parent/guardian be involved in providing information for clients who are minors. For example, a guardian will typically fill out intake forms, provide medical history, and consent to treatment on behalf of the child.

We only collect information about a child that is necessary for their treatment and well-being. Parents and guardians should ensure that any personal information children provide to MMT (such as during a session or via an online form) is given with adult supervision and consent. MMT handles children's information with the highest degree of confidentiality and security, and in accordance with all legal requirements. Where a child is mature enough to have a say in their health decisions, we involve the child in the process as appropriate, but still require parental consent for any decisions about their information for those under 18.

5.4 Consent for Sensitive Information:

Given the nature of our services, much of the personal information we collect is **health information**, which is classified as sensitive. We will seek your consent to collect and use your health information where required. By engaging our services and agreeing to our terms (for example, signing a service agreement or consent form), you are generally providing consent for us to collect and use your personal and health information to deliver care. In some cases (such as collecting details about your health history or medical reports), we may ask for written consent. If you are an NDIS participant, the service agreement or consent in your NDIS plan process may cover our collection and sharing of relevant info with NDIS-related parties. For children, a parent or guardian's consent is required.

We will only collect sensitive information without consent in exceptional situations allowed by law – for example, if it is necessary to prevent a serious threat to someone's life or health and you (or your guardian) cannot give consent, or if we are required by law to collect certain information. Outside of such rare cases, we will always endeavor to get consent first for handling sensitive personal data.

6. Use of Personal Information

6.1 Primary Purpose – Providing Physiotherapy Services:

We use the personal and health information we collect primarily to deliver and manage our physiotherapy services to you. This includes:

- **Assessment and Treatment:** We review your health information (medical history, assessment results, etc.) to plan and provide appropriate therapy or exercise programs.
- **Service Delivery:** To carry out in-person therapy sessions in Western Australia or online sessions for our remote/international clients, including tailoring our approach based on your needs and goals.

- **Care Coordination:** If you have other healthcare providers, support coordinators, or are part of a broader care team, we may use your information to communicate and coordinate with those parties (with your consent) to ensure integrated care. For example, we might use your therapy progress notes to update your GP or discuss your needs with your NDIS support coordinator.
- **Scheduling and Appointments:** Using your contact information to schedule appointments, send reminders or updates about session times/changes, and manage our therapists' schedules. Our practice management system (Cliniko) helps us organize this scheduling and may send automated appointment reminders to you via SMS or email on our behalf.
- **Billing and Administration:** Using your personal information for administrative tasks such as generating invoices, processing payments, and managing accounts. For instance, we use Stripe to process credit card payments, and your name and email may be used to send you payment links or receipts. If you are NDIS-funded, we use your details to issue invoices to you or your plan manager and to record payments.
- **Communication with You:** We may use your contact details to communicate with you about your care – for example, sending exercise instructions, follow-up advice, responding to your inquiries, or notifying you of any changes to services (like clinic policies or telehealth platform updates).

6.2 Secondary Purposes:

In addition to the core service delivery, we may also use your information for related secondary purposes that you would reasonably expect, including:

- **Quality Assurance and Training:** Internally reviewing your case (confidentially) to ensure we are maintaining high standards of care. This could involve senior practitioners reviewing treatment plans or outcomes. Any training or case review is done without identifying information where possible, or with strict confidentiality.
- **Service Development and Planning:** Using aggregated and de-identified information to help improve our services. For example, analysing what types of conditions we treat most often to develop better programs. (If we ever wish to use your identifiable information for testimonials, case studies, or marketing, we will seek your explicit written consent.)
- **Legal and Regulatory Compliance:** Using or disclosing information as needed to fulfill legal obligations. For instance, keeping adequate health records as required by health regulations, or providing information to comply with government requirements (such as mandatory reporting obligations, or providing statistical data to the NDIS or health authorities in line with the law).
- **Handling Complaints and Inquiries:** If you make a complaint through our formal process or ask us a question, we will use your information to investigate and respond, and to improve our practices if necessary.

We will not use your personal information for purposes unrelated to our services unless we have your consent or an applicable legal exception. We do **not** sell or rent personal information to any third-party for marketing or any other purpose.

If at any time you would prefer not to receive certain communications from us (for example, newsletter emails or general service announcements, if we send them), you can opt out by contacting

us (see Contact section below). Note that communications directly related to your care or appointments are not optional – we will continue to contact you as needed for these primary purposes unless you discontinue our services.

7. Disclosure of Personal Information

MMT understands that you trust us with your information and we will only disclose it to third parties in ways that respect your privacy. We do not share your personal or health information with others except in the situations described below. In all cases, we only disclose the minimum information necessary and in accordance with the law and professional ethical standards.

7.1 Disclosures for Service Provision (Routine Disclosures):

There are certain third parties we may need to share your information with in order to provide you with our services or to coordinate your care, including:

- **Your Healthcare Providers:** With your consent, we may share relevant information with your other healthcare providers. For example, we might send a report to your referring GP, discuss your progress with a specialist or another therapist involved in your care, or provide information to a hospital or medical imaging service if further investigation is needed.
- **Authorized Representatives:** If you have a legal representative, guardian, or substitute decision-maker (for example, a parent for a child, or someone holding Power of Attorney for an individual), we will share information with them as appropriate and with consent. For child clients, parents/guardians will naturally receive information about the child's treatment and progress.
- **NDIS Plan Managers and Support Coordinators:** For NDIS participants, we may share necessary information with your plan manager or support coordinator to enable services and payments. For instance, we send invoices or service agreements containing your name, NDIS number (if applicable), and service details to your plan manager for payment processing. We might also discuss your service schedule or support needs with your support coordinator to ensure our therapy aligns with your NDIS plan goals. These disclosures are only done with your (or your guardian's) understanding as part of your NDIS service arrangement.
- **Payment Processors:** As noted, if you pay by credit card or online payment, your payment details are handled by a secure third-party processor (Stripe). Stripe will receive the necessary billing information to process the transaction (such as your name, card details, and payment amount). Stripe is a third party, but this disclosure is inherent in processing the payment you have authorized. We ensure that Stripe is PCI-DSS compliant and protects your payment data; we do not keep your full card details.
- **Service Delivery Platforms:** We use certain trusted software and cloud service providers to run our operations. Personal information may be stored with or transit through these providers as part of our service to you:
    - **Cliniko (Practice Management System):** We use Cliniko to manage appointments, clinical notes, and client records. Information you provide (contact details, health history, appointment notes) is stored in Cliniko's secure cloud database. Cliniko's servers may be located in Australia or overseas; however, Cliniko is a reputable service that complies with privacy requirements.

- **Microsoft 365 OneDrive:** We may store documents or reports that contain personal information (for example, assessment reports, exercise programs, invoices) on OneDrive, which is a secure cloud storage provided by Microsoft. This allows our team to access necessary documents from various locations while maintaining security. Microsoft's data centers could be outside Australia; if so, we rely on Microsoft's high security standards and ensure any overseas storage complies with Australian Privacy Principle 8 (cross-border data protection).
- **Communication Tools:** If we use other tools (e.g. email via Microsoft Outlook, or telehealth video platforms), your information may pass through those systems in the course of communication. We choose reputable providers that employ encryption and security.

All third-party service providers we use are engaged under agreements that oblige them to protect personal information in line with privacy laws. We take reasonable steps to ensure that these providers will not use or disclose your information except to the extent necessary to provide services to us (and by extension, to you). We do not authorize them to use your data for their own marketing or other purposes.

7.2 Other Disclosures with Your Consent:

If you ask us to, or explicitly consent, we may disclose your information to other third parties. For example, if you would like us to send your treatment summary to a family member, or share information with a lawyer or insurance company (e.g. for a claim), we will do so with your written or verbal consent. We may also release information to third parties in other situations with your consent – for instance, if you want to be featured in a success story on our website, we would only publish information you agree to, and likely anonymize or de-identify it unless you've permitted otherwise.

7.3 Disclosures Required or Permitted by Law (Legal Basis):

There are circumstances where we might be required or allowed under Australian law to disclose personal information without your consent. MotionMate Training will only make such disclosures in compliance with the law. These situations may include:

- **To prevent or lessen a serious threat:** If we reasonably believe it is necessary to prevent or lessen a serious and imminent threat to a person's life, health, or safety, or to public health or safety, we may share information with authorities or medical personnel. For example, in a medical emergency during a session, we might provide critical health information to ambulance staff.
- **Required by law or court order:** If a court, tribunal, regulatory authority (such as the NDIS Quality and Safeguards Commission), or legislation compels us to produce certain information, we must comply. For example, we might receive a subpoena or notice to produce client records as part of legal proceedings. We will verify the legitimacy of any such request and only provide the minimum information required.
- **Law enforcement and national security:** We may disclose information to police or other enforcement agencies if required by law (e.g. in response to a warrant or to report a suspected crime), or to assist authorities in locating someone or preventing a crime. Additionally, if an Australian government security agency lawfully requires access (this is highly unlikely in our context), we may be obligated to provide it.

- **To protect legal rights:** We might disclose information to our legal advisors or insurers if that information is necessary to address a legal issue involving MMT (for instance, defending against a legal claim). These parties would be bound to keep the information confidential.

Where any disclosure is made under these conditions, we will document it and ensure it is done in line with the relevant APPs and Privacy Act provisions. If the law permits us to, we will also try to inform you of such disclosures (for example, if your information was sought under a court order, we may tell you unless legally restricted from doing so).

7.4 Cross-Border Disclosure:

MotionMate Training is based in Australia, and we aim to store personal information on secure servers located in Australia wherever possible. However, some of our third-party service providers (such as Microsoft or Stripe) or communication methods may involve servers in other countries (for example, data might be backed up in another region). When we transfer or store personal information outside Australia, we take reasonable steps to ensure that the overseas recipient protects the information to the same standard as required under Australian Privacy Principles. We do this by using reputable providers with robust privacy and security practices and, if necessary, by contractually obliging them to comply with Australian privacy laws or equivalent standards.

We will not send your personal information to overseas recipients unless: (a) it is necessary for the services we provide you (e.g. using the cloud software mentioned), (b) we have your consent, or (c) we are otherwise satisfied that the recipient will handle the information in a manner consistent with the APPs or a relevant exception under the Privacy Act applies. Currently, known countries where data **may** be stored or processed through our service providers include (but may not be limited to) the **United States** and **countries in the European Union** (due to global cloud infrastructure), as well as within **Australia**. If you would like more information about overseas data storage in relation to your personal information, please contact us.

8. Data Security and Storage Practices

MotionMate Training takes the security of personal information very seriously. We employ a combination of administrative, technical, and physical safeguards to protect the personal and health information we hold from misuse, interference, loss, and unauthorized access, modification or disclosure.

8.1 Secure Storage:

- **Electronic Records:** The majority of client personal information is stored electronically. We use secure, password-protected systems such as Cliniko (for clinical records and scheduling) and Microsoft OneDrive (for documents) to store your information. These systems employ industry-standard security measures, including encryption, to protect data at rest and in transit. Access to these systems is restricted to authorized MMT personnel on a need-to-know basis. Each staff member has unique login credentials, and where available, multi-factor authentication is enabled for added security.
- **Payments:** Payment information entered via Stripe is transmitted securely using encryption (SSL/TLS). Stripe maintains its own stringent data security standards (PCI-DSS compliance). MMT does not keep your credit card details – any saved payment information is stored by Stripe, not on our local systems.

- **Hard Copies:** We operate predominantly in a digital format. However, if any paper documents containing personal information are created (for example, signed consent forms, or printed exercise programs), we keep them in a secure manner (e.g. a locked filing cabinet in a restricted office area). We discourage keeping paper records unless necessary. If traveling to appointments, our therapists carry only the information needed and keep it secure (for instance, using locked bags or device security for laptops/tablets).
- **Emails and Communication:** When communicating via email or other electronic means, we use secure company accounts. However, email is not always fully secure; for sensitive information, we may use encrypted files or secure portal links when necessary. We advise clients to be cautious in sending highly sensitive details to us via regular email; we can provide a secure method if needed.
- **OneDrive and Cloud Files:** Any documents stored in cloud storage (OneDrive) are only accessible to MMT staff and protected by Microsoft's security protocols. We organize files so that only the relevant staff (for example, your therapist and necessary administrative staff) can access your specific documents.

8.2 Data Security Practices:

- **Staff Training and Policies:** All MMT staff are trained in confidentiality and privacy requirements. We have internal policies to ensure staff handle personal data properly – this includes securing devices, not sharing login credentials, and being vigilant about phishing or other security threats.
- **Device Security:** Any laptop or tablet used to access personal information is password-protected and has updated antivirus/anti-malware software. Mobile devices are set to auto-lock and can be wiped remotely if lost.
- **Network Security:** Our digital systems employ firewalls and encryption. When accessing records remotely (since we are a mobile service), staff use secure internet connections and/or VPNs to avoid unauthorized interception of data.
- **Monitoring and Auditing:** We keep audit logs of access to electronic records where possible (for example, Cliniko logs user access to client files). We periodically review these logs to ensure that only appropriate access is occurring.
- **Third-Party Security:** We vet our third-party service providers for their security standards. For example, Microsoft and Stripe are large organizations with robust security programs. Cliniko is a health practice management platform known for catering to Australian practitioners and is designed with privacy compliance in mind. If we consider any new system or provider, we assess its security and privacy measures before use.

Despite all our efforts, it's important to note that no method of electronic storage or transmission is 100% secure. However, MMT strives to use industry best practices to minimize the risk of unauthorized access to or disclosure of your information. In the unlikely event of a data breach that is likely to result in serious harm (for example, a cyber-attack leading to theft of personal data), we will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as required by the **Notifiable Data Breaches** scheme under the Privacy Act.

8.3 Data Retention and Disposal:

We retain personal information for as long as it is needed for the purposes described in this policy, or

as required by law, whichever is longer. Health records often must be kept for certain minimum periods under healthcare regulations (for example, adult health records are commonly kept for 7 years from last entry, and records of minors kept until the child turns 25). We adhere to such requirements. When personal information is no longer required and is not required to be retained by law, we take reasonable steps to destroy it or de-identify it securely. This could involve permanent deletion of electronic files and backups, and shredding or secure destruction of any paper records.

9. Data Quality and Client Rights

9.1 Data Quality (Accuracy of Information):

We rely on the information provided by you (or your representatives) to be accurate, complete, and up-to-date. We take reasonable steps to ensure that the personal information we collect, use, or disclose is correct and up-to-date. This includes updating our records when you inform us of a change (for example, if you have a new address or phone number, or a change in medical condition). We may also verify details with you from time to time (such as confirming your contact information or checking that we have the correct emergency contact on file). We encourage you to let us know if any of your information changes or if you believe any information we hold is inaccurate or incomplete.

9.2 Right to Access Your Information:

You have the right to request access to the personal information that MotionMate Training holds about you, in accordance with APP 12 and the Privacy Act. For example, you may request to see the records of your treatment or the contact details we have on file. To make an access request, please contact us using the details in the Contact section below. We will need to verify your identity (to ensure we don't give your information to someone else). For requests involving a child's records, we will verify that you are the parent or legal guardian or otherwise authorized.

Once we have sufficient details and verification, we will provide you with access to the information requested, where it is reasonable and practical to do so. We will usually provide the information in the format you request (for instance, a printout or electronic copy), or otherwise in a suitable format such as a summary letter, depending on the nature of the request. We will respond to your request within a reasonable time frame (generally within 30 days).

There is no fee for making an access request. We may charge a reasonable fee to cover administrative costs (for example, if a large volume of copying is required), but we will let you know in advance and such fees will **not be excessive**. We will not charge for simply lodging a request.

In some situations, we may **deny or limit access** as permitted by law. Reasons we might refuse access include circumstances where:

- Providing access poses a serious threat to the life, health or safety of any individual, or to public health or safety (for example, if releasing certain information would likely cause harm to the client or someone else);
- Providing access would have an unreasonable impact on the privacy of other individuals. (for example, if the information also contains references to another person who has not consented);
- The request is frivolous or vexatious (e.g. repeated requests with no serious purpose);
- The information relates to existing or anticipated legal proceedings between you and MMT, and would not be accessible through the process of discovery in those proceedings;

- Providing access would reveal our intentions in relation to negotiations with you in a way that prejudices those negotiations;
- Providing access would be unlawful (we are prohibited by law from giving it); or
- Denying access is required or authorized by law (for example, under certain regulations we may be prevented from releasing information).

If we refuse access to any part of your request, we will provide you with written reasons for the refusal and the legal basis for it, except where it would be unreasonable to do so. We will also let you know if there are any other ways to obtain the information (or a summary of it). In some cases, if direct access is not appropriate, we may offer to provide the information through a health professional (for example, if it's health information that should be explained by a practitioner) or offer another intermediary solution.

9.3 Right to Correct Your Information:

You have the right to request correction of personal information that you believe is inaccurate, out-of-date, incomplete, irrelevant, or misleading. If you notice an error in your personal details or records, please inform us. We will take reasonable steps to correct the information as soon as practicable, in line with APP 13.

If it is something straightforward (like updating a phone number or correcting a misspelling), we will make the change upon verification. If we disagree that the information is incorrect (for example, if our professional opinion recorded in a health record is challenged), we will let you know our reasons. In such cases, you have the right to request that we associate a statement with the record noting your disagreement or the correct information that you believe should be recorded. We will take reasonable steps to do this so that it is apparent to anyone accessing the record in the future that you believe certain information is not accurate.

We will not charge you for requesting a correction. We will notify you when we have corrected the information, or if we refuse to correct it, we will provide you with the written reasons for refusal and information on how to complain if you are not satisfied.

9.4 Withdrawing Consent:

Where you have provided consent for us to use or disclose your personal information, you have the right to withdraw that consent at any time. For example, if you previously gave consent for us to share information with a particular third party and you no longer want that to happen, you can let us know to cease that sharing. To withdraw consent, please contact us. We will explain any consequences of withdrawing consent – in some cases, withdrawing consent for us to use certain information may mean we are unable to continue to provide certain services to you.

If you withdraw consent for a secondary use of information (such as receiving a newsletter or participating in a case study), it will not affect the core services we provide. We will promptly action your withdrawal request and confirm once we have ceased the relevant use or disclosure. Note that withdrawal of consent will not affect any use or disclosure that has already occurred with your prior consent.

10. Complaints and Further Information

MMT is dedicated to addressing any concerns or complaints regarding privacy promptly and fairly. We view complaints as an opportunity to improve our practices. If you believe that we have breached

your privacy or this Privacy Policy, or if you have questions about how we handle your personal information, please do not hesitate to contact us.

10.1 How to Contact Us:

- **Email:** chad.mclean@motionmatetraining.com.au
- **Phone:** (+61) 437 877 553 (Australian mobile number)

When you contact us with a privacy query or complaint, please provide as much information as possible about your concern (for example, the date of the incident, what you believe went wrong, and any relevant context). Our Privacy Officer or another designated person will acknowledge your complaint and seek to understand and resolve the issue. We may request additional details or clarifications from you during our investigation.

10.2 Our Complaints Handling Process:

Upon receiving a privacy complaint, we will:

- Acknowledge receipt of the complaint promptly (generally within 5 business days).
- Investigate the complaint, which may involve reviewing relevant records, speaking with the involved staff, and assessing our procedures against the concern raised. We will treat the process confidentially.
- Respond to you with the outcome of the investigation and any actions we will take to address the issue. We aim to provide a substantive response within 30 days. If the matter is complex or requires more time, we will let you know and keep you informed of the progress.
- If a mistake was made or a breach occurred, we will inform you of the steps we are taking to rectify it and to prevent it from happening again. Where required, we will also report the incident to authorities (for example, if it's a notifiable data breach).

If you are not satisfied with our response, you have further options:

10.3 Escalation – External Avenues:

We hope to resolve any privacy concerns directly. However, if you feel that we have not adequately addressed your complaint, you have the right to escalate the matter to external authorities:

- **Office of the Australian Information Commissioner (OAIC):** The OAIC is the federal agency overseeing privacy laws. You can contact the OAIC to make a complaint about an interference with your privacy. The OAIC's contact details are:
    - Website: **oaic.gov.au** (which provides an online complaint form and email contact)
    - Phone: **1300 363 992**
    - Email: **enquiries@oaic.gov.au**
    - Mail: GPO Box 5218, Sydney NSW 2001, Australia.

The OAIC generally expects that you have given the organisation (MMT) a chance to respond to your complaint first, before they will investigate, so please contact us before reaching out to OAIC.

- **NDIS Commission (for NDIS participants):** If your concern relates specifically to how we handled your information as a NDIS service provider, you may also contact the NDIS Quality and Safeguards Commission. They oversee providers' compliance with the NDIS Code of

Conduct and other standards, which include respecting participant privacy. The NDIS Commission's contact is **1800 035 544** or via their website **ndiscommission.gov.au**.

- **State Privacy or Health Ombudsman:** In Western Australia, certain health privacy complaints can be directed to the WA Health Ombudsman or Privacy Commissioner (though federal Privacy Act usually covers us as a private organisation). We can assist in directing you to the appropriate body if needed.

We value your feedback and take your privacy rights seriously. We will not penalize you for raising a privacy concern. Your services with us will not be affected because you lodge a complaint in good faith.

11. Changes to This Policy

MotionMate Training may update this Privacy Policy from time to time to reflect changes in our practices, feedback from clients, or changes in legal requirements. When we make changes, we will update the "Effective Date" at the top of the policy. If changes are significant, we may also inform our clients directly (for example, via email or a notice on our website). We encourage you to review this policy periodically to remain informed about how we protect your personal information.

We maintain previous versions of our Privacy Policy for record-keeping and you may request a copy of an earlier version if needed.

12. Version and Review

Version: 1.0
Effective Date: 06/01/2026 (6th January 2026)
Next Review Due: January 2027 – (MotionMate Training will review this Privacy Policy on an annual basis, or more frequently if required by changes in law or our practices, to ensure it remains accurate and compliant.)

This Privacy Policy is designed to provide comprehensive information in a clear manner. If you require any clarification on the terms used or the intentions of any section, please contact us.