

Your local support team
Speech Pathology
Occupational Therapy
Music Therapy
Group Programs



Unit 11, 9-13 Princeton st
Kenmore, 4069
hello@amazetherapy.com
0436 276 590
ABN: 60 655 001 675

Privacy Policy (Last Updated Dec 2025)

Privacy Policy is an excerpt from the Amaze Children's Therapy Services Operational Handbook.

10.6. Privacy Policy

10.6.1. Policy Statement

Amaze Therapy is dedicated to protecting your privacy. We manage, use and store data in accordance with the Australian Privacy Principles (APPs) outlined in the Privacy Act 1988 (Cth), the Privacy and Personal Information Act 1998 (NSW), the Privacy and Data Protection Act 2014 (Victoria), Information Privacy Act 2009 (Qld), Hospital and Health Boards Act 2011 (Qld) and the Health Records and Information Privacy Act 2002. This policy explains how we handle your information.

Privacy and the National Disability Insurance Scheme

Privacy is a human right, and we respect the privacy of people with a disability. People with a disability have a right to privacy, including in relation to the collection, use and disclosure of information concerning them and the services they receive. As an allied health provider working with clients under the NDIS, we are subject to the NDIS Code of Conduct (2019) (the NDIS Code).

Amongst other things, this means we must:

- respect and protect the privacy of everyone that receives supports and services from us and our workers;
- manage health information about any people we support and our workers in accordance with privacy laws related to the management of health information; and
- have this Policy and provide you with this Notice about our privacy policy and procedures to help ensure we (and our workers) understand our obligations.

We are committed to treating you in a dignified way that maintains your personal privacy

Privacy is about more than simply meeting our legal obligations. It is also about the way we deliver our services to people with a disability. We will work hard to be aware of your privacy needs and preferences and will deliver our services in a way that maintains your personal dignity. Without limiting what we mean by this commitment, we will:

- explain and request your permission to perform procedures that involve physical touch or the invasion of your personal space;
- provide services in a timely manner to prevent your embarrassment and discomfort, e.g. such as toilet breaks

What, specifically, are this Policy and Notice about?

In this Policy and Notice, we explain:

- the kinds of personal information that we collect and hold, including recorded audio and visual materials;
- why we hold this information;
- who will have access to this information;
- how we ensure that information is secure;
- how we use the information;
- how you can access and amend information held about you; and
- how to make a complaint if you feel that we have breached our privacy obligations to you.

When we refer to "clients" or "you" below, we mean both former and current clients, as well as people who make inquiries about our products and services (i.e. potential clients).

10.6.2. Collecting Your Information

We collect personal and clinical information fairly and transparently. This includes:

- names, ages, dates of birth, genders, and other identifying information;
- Medicare and health fund details (including Medicare numbers and health fund insurers and the extent of their coverage);
- developmental, medical, ethnic, language, cultural and social histories (including medications, diagnoses, surgeries, and allergies);
- details about disabilities, impairments, challenges, barriers and facilitators;
- family histories, to the extent they may be relevant to our services;
- work and education histories;
- hobbies, motivations, interests, and activities in which clients and their families like to participate;
- financial information concerning the ability of clients to pay for our products and services;
- details related to the NDIS, including details of negotiations, assessments, plans and packages;
- call records, wireless locations, and unique web browser details (when you use our products and services, including online services).

For sensitive information – such as information about your health that is reasonably necessary for us to provide you with services or products – we will seek your informed consent.

Client information is used strictly for the purpose of providing individualised therapy services and care. We only disclose information to third parties when necessary for treatment, with client consent, or as required by law. Our staff are trained to always handle information discreetly and respect client confidentiality.

Information collected during assessments and therapy sessions follows the guidelines of Australian Privacy Principle 10.

10.6.3. How We Collect Information

We collect information openly and transparently, following Australian Privacy Principle 1. We gather information through:

- Direct interactions with you, such as during assessments and therapy sessions, including in person, by telephone or email
- Secure online platforms for communication and scheduling.
- Permission-based sharing of information from third parties like healthcare providers and teaching staff
- via our website when you use our networks, products and services, including our online services;
- via pages on our social media sites;
- through our client questionnaires;
- by written letters, reports and other documents (e.g. through reports you provide to us);
- through emails, SMS and other forms of electronic communication;
- in interviews and other interactions with you (including face-to-face interviews and interviews conducted electronically, such as by way of Skype, Zoom, or other means); and
- by taking notes and making recordings of our interactions with you (including audio and visual recordings).

We collect personal information from clients or someone authorised to act on the behalf of clients (e.g. their parents, carers or guardians). Wherever practicable, we will ask for the information directly. However, we may need to contact others when relevant to a client's circumstances (e.g. when working with clients who cannot communicate their needs without the assistance of others). In these cases, we will, when practicable, make you aware of the fact that we have collected this information and the circumstances of the collection.

When you give us information about other people, we rely on you to have obtained their prior consent and we expect that you tell them of the types of third parties we may provide the information to and why.

10.6.4. Using Your Information

We collect personal information to deliver, review and improve the products and services that we provide. Generally, these services and products relate to the delivery of allied health services. If we didn't collect this information, we wouldn't be able to carry out our business or provide services to you in accordance with the standards required by law, the NDIS Code, or our professional ethics requirements. If you do not provide the personal information that we request, we would not be able to carry out our business and provide our products or services to you.

More specifically, we need personal information (including health information) to provide clients with assessment, diagnosis and the provision of allied health services. We also need this information:

- for administrative purposes of managing our business;
- when necessary, to fulfil our obligations under law, regulation, the NDIS Code and/or our professional ethics rules;
- for billing management (either directly or through insurers or other compensation agencies);

- for discussions between workers related to the care of clients;
- for discussions and other communications, e.g. with your doctors, other health professionals, and others related to your care;
- for discussions with insurers (including the NDIS and its agents);
- for any insurance or compensation or other claims or litigation (including threatened litigation);
- for security and workplace safety purposes, e.g. to monitor the safety of participants, workers and others; and

From time to time, we may use personal information (but not sensitive health information) to provide you with news or offers about our products or services that may be of interest to you. We will ensure that your consent to receive this type of communication from us is opt-in, affirmative and freely given. These products and services will be related to our services described above and will be products and services that we believe will be relevant to you.

You have a right, at any time, to tell us that you don't want to receive this type of material.

Due to the nature of our services and products, we cannot offer them to people who wish to be anonymous, wish to use a pseudonym or who do not provide us with enough information to properly identify them for the purposes of providing services and products.

10.6.5. Keeping Your Information Safe

We know that you are concerned about your personal information – especially your health information. Following Australian Privacy Principle 11, we will use reasonable endeavours to prevent unauthorised access to, modification of, disclosure, misuse, or loss of that information, except as required by law (e.g. under mandatory reporting laws, and our obligations to report incidences of violence, exploitation, neglect and abuse, and sexual misconduct to the NDIS Quality and Safeguards Commission and the police).

Our directors and staff have reviewed the requirements of the Privacy Laws and our third-party service providers are aware that they are required to comply with the requirements of the Privacy Act 1988 (Cth).

We have data protection measures in place (including password-locked computers) when we access and store personal information electronically. Our measures include:

- Secure electronic storage with restricted access
- Regular security assessments
- Ongoing staff training on privacy and security practices

We use the Splose practice-management platform to create, store and manage all client records, appointment notes, invoices and communications. Splose is an Australian-owned, cloud-based system purpose-built for allied-health and NDIS providers.

Why we trust Splose

Australian data residency: All production data for Australian workspaces is housed in AWS data-centres located in Australia, ensuring compliance with federal and state data-sovereignty expectations.

Strong encryption: Data is protected with TLS/SSL while in transit and AES-256 encryption at rest.

Redundant, hourly backups: Encrypted backups are replicated across multiple AWS availability zones for high availability and disaster recovery.

Granular access controls: Role-based permissions, mandatory strong passwords, optional two-factor authentication (2FA) and SSO via SAML/OIDC help prevent unauthorised access.

Comprehensive audit logging: Every log-in, record edit and file upload is recorded so that any access or change can be traced.

The full Splose security overview is available at <https://splose.com/resources/security>, and the current privacy policy is at <https://splose.com/privacy-policy>.

Your information (though not clinical information) may also be stored within the Google Workspace environment. This information is password protected, accessible only to members of AmazeTherapy and encrypted and protected in line with Google's own cloud storage standards.

Use of Heidi AI

To streamline record-keeping and improve the accuracy of our session notes, our clinicians may use Heidi AI, an Australian-hosted artificial-intelligence tool that converts brief audio recordings and typed prompts into a draft clinical note. Heidi is used only for the direct purpose of providing therapy services and never to make automated care decisions.

Key points you should know

What happens	Your safeguards
Data in – short audio clips or keywords captured during or immediately after your appointment	Transmitted via encrypted (TLS) channels to Heidi's Australian data-centre, then deleted once the draft is prepared
Data out – a draft transcript and summary	Reviewed, edited and approved by a registered allied health professional before being saved to your permanent file in Splose
Security	AES-256 encryption at rest, role-based staff access, full audit logs; Heidi data is not used to train public AI models
Retention	Audio is purged after transcription; approved notes are stored in Splose for at least 7 years (or until a minor turns 25) in line with professional requirements

What happens	Your safeguards
Your choice	AI assistance is optional—tell your clinician at any time if you prefer manual note-taking

10.6.6. Access and Correction

You have the right to access and correct your information, as per Australian Privacy Principle 12. We take reasonable steps to ensure that personal information we collect about or from you is accurate, complete, up-to-date and relevant whenever it is used, collected or disclosed.

Subject to the recognised exceptions to access for organisations contained in the Australian Privacy Principles (APP12.3), you have a right to access your information if you wish (subject to any privilege or legal restrictions); and, if it is reasonable and practicable to do so, we will give you access to the information in the manner requested by you. By law, we may charge you a reasonable fee to cover the cost of retrieving and processing the information.

If you believe personal information that we hold about you is inaccurate, out-of-date, incomplete or misleading, we will, on receipt of your request, take steps that are reasonable in the circumstances to correct the information.

Your information may be seen or used by people working for or on behalf of us and other service providers including (without limitation)

- our directors and owners;
- our professional workers (employed or contracted);
- our administrative staff (employed or contracted);
- our third-party professional advisors and service providers, including (without limitation) our lawyers, book-keepers, accountants, auditors, tax consultants, actuaries, management consultants and IT service providers (including software-as-a-service providers);
- Medicare, private health insurance providers, our insurers and reinsurers;
- the National Disability Insurance Agency and its agents.

We will not rent, sell, trade or otherwise disclose to any other third parties any personal information about you without your consent, or unless we are required to by law (including pursuant to a court or tribunal order), or where a permitted general situation (including a permitted health situation) exists within the meaning of the Privacy Act 1988 (Cth), or if we reasonably believe disclosure is necessary for enforcement-related activities.

10.6.7. Retaining Your Information

We keep your information only as long as necessary, aligning with Australian Privacy Principle 4. When no longer needed, we securely destroy or de-identify it.

Clinical information shared with us will be retained securely until a child reaches 25 years of age or, for an adult, a period of 7 years after that person turns 18 years old, as required under Australian Law. At

the expiry of this period, it will be variously destroyed or deleted and will no longer be accessible to any person.

10.6.8. Sharing with Third Parties

We share your information with third parties like healthcare providers and educators only when needed for therapy services or with your consent, following Australian Privacy Principle 6 and Principle 8.

It is a condition of service that clients obtain written permission from the therapist prior to

- making any recordings of the session, whether that session be undertaken in person or via telehealth, and
- prior to sending such recordings to, or sharing them with, any other party.

Information about webinars, seminars and courses

We may offer webinars, seminars and training courses on a range of topics to you and others in the course of our business relationship with them. These are part of our business and business development efforts.

If you sign up to a seminar, webinar, or course, we will process your registration data (including your name and email address) to administer access and to prepare and present the webinar, seminar or course (as the case may be). We will also use your registration data for the purposes of our business development.

Information about social media plug-ins

To improve the quality of our services to clients, our website includes social media plug-ins of the large social media networks, including [Instagram, Twitter, Facebook, and LinkedIn]. Upon opening a website on which a social media plug-in is embedded, the social network provider will collect and process information on your visit to our website for its own business purposes. This is not initiated or controlled by us, but is a built-in feature of most social media plug-ins. For further information about these plug-ins and privacy, refer to the social media platform's privacy policy.

10.6.9. Cross-Border Sharing

Excepting the exclusions outlined in the Cloud Based Computing Policy, if we share your information across borders, we will take all reasonable steps to ensure it complies with Australian Privacy Principles 8 and 11. We will share this data across borders as outlined in the Cloud Based Computing Policy, or at the request of Australian law enforcement.

10.6.10. Privacy Concerns

If you have concerns about your privacy, let us know. We take privacy seriously, and we'll address any complaints promptly and thoroughly.

Complaints and asserting your privacy rights

If you believe your privacy has been prejudiced by something we have done or failed to do, you have a legal right to lodge a complaint. If you make a complaint to us, our Privacy Officer will treat it very seriously, and will handle your complaint per our Client Complaints Policy.

Our Privacy Officer is Karina Cook, who can be contacted by phone at 0434 974 971, email at karina@amazetherapy.com and in writing via 11/9-13 Princeton Street, Kenmore, QLD 4069. In any event, we will respond to you in writing within 15 days of receiving your complaint.

A breach of your privacy may constitute a breach of the NDIS Code. In this situation, you or anyone can make a complaint to us, or to the NDIS. As suggested in the NDIS Code, we encourage you to contact us first, to see if we can resolve the matter directly.

You also have the right to lodge a complaint with the Office of the Australian Information Commissioner, who is the competent supervisory authority.

A breach of privacy by a professional who works for us (e.g. a health care worker) may also be a breach of their professional code of conduct or code of ethics.

As noted above, you have several statutory rights under privacy laws, including rights to information, access, rectification and the withdrawal of your consent to the collection and use of personal information. If you wish to assert any of these rights, please contact our Privacy Officer using the contact details included above.

Want more information?

If you have any questions about this Policy or this Notice, or have any concerns about the personal information you or others have given us about you, please contact us at [insert contact details]. More information on the Privacy Act 1988 (Cth) can be found on the website of the Office of the Australian Information Commissioner: <https://www.oaic.gov.au/>

This Policy and Notice are in addition to, and do not relieve, remove or replace our rights and responsibilities under applicable laws. If there is a conflict between this Policy and this Notice, on the one hand, and an applicable law, on the other hand, the law shall prevail to the extent of any conflict.

10.6.11. Policy Updates

We regularly review and update this policy, as per Australian Privacy Principle 5. The latest version is available on our website.

10.6.12.

Australian Privacy Principles

Amaze Therapy Privacy Policy is informed by the Australian Privacy Principles. For clarity, the plain English version of these is included below. The Privacy Principle and guidelines are available here: <https://www.oaic.gov.au/privacy/australian-privacy-principles>

APP 1 - Open and Transparent Management of Personal Information:

- Organisations must have a clear and transparent policy for managing personal information. Individuals should be aware of how their information is handled.

APP 2 - Anonymity and Pseudonymity:

- Where possible, individuals have the option to remain anonymous or use a pseudonym when dealing with an organisation, unless it's impractical or required by law.

APP 3 - Collection of Solicited Personal Information:

- Organisations must only collect personal information that is reasonably necessary for their functions or activities, and they must do so by lawful and fair means.

APP 4 - Dealing with Unsolicited Personal Information:

- If an organisation receives unsolicited personal information, they must determine whether it could have collected it under APP 3. If not, the information must be destroyed or de-identified.

APP 5 - Notification of the Collection of Personal Information:

- Individuals must be notified about the collection of their personal information, including the purpose for collection, who it may be disclosed to, and other relevant details.

APP 6 - Use or Disclosure of Personal Information:

- Organisations can only use or disclose personal information for the primary purpose for which it was collected, unless the individual consents or the law allows.

APP 7 - Direct Marketing:

- Personal information must not be used for direct marketing purposes unless the individual consents or it is impractical to seek consent.

APP 8 - Cross-Border Disclosure of Personal Information:

- Before disclosing personal information overseas, organisations must take reasonable steps to ensure that the recipient complies with the APPs, unless an exception applies.

APP 9 - Adoption, Use, or Disclosure of Government Related Identifiers:

- Organisations must not adopt, use, or disclose government-related identifiers (e.g., driver's license numbers) unless required by law or necessary for verification purposes.

APP 10 - Quality of Personal Information:

- Organisations must take reasonable steps to ensure that the personal information they collect is accurate, up-to-date, and complete.

APP 11 - Security of Personal Information:

- Organisations must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure.

APP 12 - Access to Personal Information:

- Individuals have the right to access their personal information held by an organisation and request corrections if it is inaccurate.

APP 13 - Correction of Personal Information:

- If an individual requests a correction to their personal information, the organisation must take reasonable steps to correct it unless certain exceptions apply.

These definitions provide a broad overview of each Australian Privacy Principle. For more detailed and legal-specific information, it is advisable to consult the full text of the Privacy Act 1988 (Cth) or seek legal advice.

This Policy has been informed by the following:

- the Privacy Act 1988 (Cth) (“Privacy Act”) (including the Australian Privacy Principles under that Act);
- Relevant Queensland legislation such as the Hospital and Health Boards Act 2011 (Qld) (public-sector disclosure offences) and general obligations under the Health Practitioner Regulation National Law (Queensland);
- Speech Pathology Australia Code of Ethics (2020) and AHPA *Keeping health records* guidelines – including the minimum retention period of 7 years after the last date of service (or until a minor turns 25).
- NDIS Practice Standards & Quality Indicators (2021), for providers who deliver NDIS-funded services (record-keeping, information-security and privacy requirements), and
- marketing legislation, including the Spam Act 2003 (Cth) and the Do Not Call Register Act 2006 (Cth)