



Privacy Policy

Australian allied-health and NDIS practice

Legal entity	Speechie Steph
ABN	63 772 487 561
Effective date	12 July 2026
Policy owner	Privacy Officer / Principal Speech Pathologist

Contents

- 1 About this policy
- 2 Who we are and who the policy applies to
- 3 Privacy framework
- 4 Information we collect and hold
- 5 How we collect information
- 6 Why we collect, hold, use and disclose information
- 7 Consent, capacity and client choice
- 8 When we disclose information
- 9 Splose and other digital service providers
- 10 Reports, clinical records and business devices
- 11 Email, SMS, online bookings and telehealth
- 12 Audio, video and AI-assisted documentation
- 13 Overseas processing and disclosure
- 14 Data quality
- 15 Security safeguards
- 16 Retention, destruction and de-identification
- 17 Accessing and correcting information
- 18 Data breaches
- 19 Direct marketing
- 20 Website, cookies and analytics
- 21 Privacy complaints
- 22 Changes to this policy
- 23 Contact details

Appendix A Short privacy collection notice for Splose

Appendix B Consent wording for intake forms

1. About this policy

Speechie Steph respects the privacy, dignity and autonomy of clients, families, carers, workers and other people whose information we handle. This Privacy Policy explains how Speechie Steph collects, holds, uses, discloses, secures, retains and provides access to personal information, including sensitive and health information.

This policy is intended to be read with any collection notice, consent form, service agreement, telehealth consent, recording consent or other notice provided at the time information is collected. A collection notice gives more specific information about a particular collection of information; this policy describes our broader information-handling practices.

2. Who we are and who the policy applies to

Speechie Steph is a speech pathology practice operating under ABN 63 772 487 561. In this policy, “Speechie Steph”, “we”, “us” and “our” refer to the practice and its authorised workers, contractors and representatives.

This policy applies to information about current, former and prospective clients; parents, guardians, nominees, carers and support people; referrers and other professionals; website visitors; suppliers and contractors; and applicants or workers where the Australian Privacy Principles apply.

3. Privacy framework

As a private health service provider, Speechie Steph handles personal and health information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles. We also comply with other applicable laws, contractual duties, professional standards and funding requirements, including relevant NDIS requirements where services are provided to NDIS participants.

Where another law imposes a higher privacy, confidentiality, recordkeeping or disclosure standard, we will apply that higher standard.

4. Information we collect and hold

We collect only information that is reasonably necessary for our functions and activities. The types of information may include:

- identity and contact information, including name, preferred name, pronouns, date of birth, address, email address, phone number and emergency contacts;
- information about a parent, guardian, nominee, authorised representative, carer or support person, including the nature and scope of their authority;
- health and sensitive information, including medical, developmental, disability, communication, speech, language, literacy, voice, fluency, feeding or swallowing history; diagnoses; medications; allergies; hearing and vision information; risk information; family, social, cultural and linguistic background; and information about support needs;
- clinical information, including referrals, intake information, consent records, assessment data, observations, case history, session notes, therapy plans, goals, progress data, reports, recommendations, correspondence and discharge information;

- education and participation information, including school, childcare, workplace, community activities, reasonable adjustments and information supplied by teachers or other support people;
- NDIS and funding information, including NDIS number, plan dates, plan management type, support categories, service bookings, nominee details, support coordinator or plan manager details and information reasonably required for service agreements, claims or reports;
- billing and transaction information, including invoices, payment status, rebates, insurer or funding information and limited payment information processed by authorised payment providers;
- communications and appointment information, including enquiries, online booking details, waitlist information, appointment reminders, emails, SMS messages, phone notes and complaints or feedback;
- images, audio or video recordings only where clinically required or otherwise agreed, and only with appropriate notice and consent unless collection is required or authorised by law;
- website and technical information, such as IP address, browser type, device information, cookies, booking-form activity and website analytics, where enabled; and
- information about contractors, suppliers, referrers and professional contacts that is reasonably required to manage business relationships.

5. How we collect information

We usually collect information directly from the client or, where appropriate, from a parent, guardian, nominee, authorised representative or support person. Collection may occur:

- through Splose online booking, referral, intake, consent, service agreement and other forms;
- during phone, email, SMS, telehealth, in-person, school, childcare, home or community interactions;
- during assessments, therapy sessions, case conferences, reviews and report preparation;
- through our website, social media pages or other communication channels; and
- through billing, payment, accounting, funding and complaint-management processes.

With consent, or where otherwise permitted by law, we may collect information from referrers, health professionals, schools, childcare services, support coordinators, plan managers, insurers, the NDIA, government agencies, family members or other members of a treating or support team.

If we receive unsolicited personal information, we will determine whether we could have collected it lawfully. If not, and if lawful and reasonable to do so, we will securely destroy or de-identify it.

6. Why we collect, hold, use and disclose information

We collect, hold, use and disclose information for purposes including:

- responding to enquiries, managing referrals, waitlists and bookings, and determining whether we can provide an appropriate service;
- confirming identity, authority, consent, safety needs, communication access needs and service preferences;
- providing speech pathology assessment, diagnosis where within scope, therapy, consultation, parent or carer coaching, education, reports, recommendations and discharge planning;

- coordinating care and communicating with authorised members of a client's treating, education or support team;
- preparing clinical notes, reports, letters, funding applications, progress summaries, service agreements, quotes and other documents requested or authorised by the client;
- managing appointments, reminders, telehealth, home, school, childcare and community-based services;
- processing invoices, payments, rebates, NDIS claims, plan-managed or agency-managed claims and debt recovery;
- managing risks, incidents, complaints, safeguarding concerns, insurance matters, legal obligations and professional responsibilities;
- quality assurance, clinical supervision, professional consultation, audit, training and service improvement, using de-identified information wherever practicable;
- maintaining secure business records, backups, cybersecurity, system administration and continuity of care; and
- complying with laws, court or tribunal orders, lawful information requests and funding or regulatory requirements.

We will not use or disclose personal information for an unrelated purpose unless the individual has consented or the use or disclosure is otherwise permitted or required by law.

7. Consent, capacity and client choice

We seek informed consent before collecting sensitive information unless an exception applies.

Consent may be express or implied depending on the circumstances, but we generally seek express and recorded consent for health information, information sharing, recordings and other higher-risk activities.

Consent must be voluntary, informed, current and specific. We avoid bundling optional consents with consent that is necessary to provide the service. A client or authorised representative may withdraw or change consent at any time by contacting us. Withdrawal does not affect actions already taken lawfully, and it may limit our ability to provide some services or coordinate care.

For children and people who require support with decision-making, we consider the person's age, maturity, capacity, preferences, communication needs, best interests, legal authority and any relevant parenting, guardianship or court orders. We involve the client in decisions to the greatest extent possible and take reasonable steps to verify who is authorised to access or disclose information.

People may make general enquiries anonymously or using a pseudonym where practical. It is generally not practicable to provide clinical services, maintain safe health records, process funding or meet legal obligations without collecting identifying information.

8. When we disclose information

We may disclose relevant information to the following people or organisations where the disclosure is reasonably necessary, expected and authorised, or otherwise permitted or required by law:

- a parent, guardian, nominee, authorised representative or support person, subject to verifying authority and considering the client's rights and safety;

- referrers and authorised health, education, childcare, disability or support professionals involved in the client's care or participation;
- support coordinators, plan managers, the NDIA, insurers, funding bodies and claims administrators for service delivery, billing, reporting, audit or funding purposes;
- Splose and contracted providers that support practice management, email, payments, banking, website hosting, information technology, cybersecurity and business administration;
- professional supervisors, consultants, legal advisers, accountants, auditors and insurers who are subject to appropriate confidentiality obligations;
- government, regulatory, safeguarding, child protection, law enforcement, court or tribunal bodies where required or authorised by law; and
- another person or organisation where reasonably necessary to lessen or prevent a serious threat to life, health or safety, or in another permitted general or health situation.

We take reasonable steps to disclose only the minimum information necessary for the purpose, verify recipient details and record significant disclosures. We do not sell client information.

9. Splose and other digital service providers

Speechie Steph uses Splose as its primary practice-management platform. Splose may be used for online bookings, referrals and forms, client records, service agreements, appointments, reminders, clinical notes, reports, invoices, NDIS-related administration and document storage. Card payments are processed through Stripe, and banking and payment settlement information is handled through ANZ.

Splose states that Australian user data is stored in Australia, encrypted in transit and at rest, backed up, and protected through account security and user-permission controls. Speechie Steph remains responsible for configuring and using its Splose workspace appropriately, controlling authorised access, maintaining secure credentials and determining what information is entered into the platform.

Speechie Steph also uses Microsoft Outlook for business email. Each provider handles information under its own privacy policy and contractual terms. We assess providers having regard to the sensitivity of the information, the service being provided, security and privacy controls, data location, access arrangements, breach processes and our legal obligations.

Speechie Steph does not use a separate consumer cloud-drive service to store client clinical records. Stripe and ANZ receive only the billing, contact and transaction information reasonably necessary to process or reconcile payments; clinical reports are not intentionally provided to Stripe or ANZ.

10. Reports, clinical records and business devices

Clinical records and reports may be created, viewed and stored within Splose and on Speechie Steph's dedicated business computer. Working copies may be downloaded from or uploaded to Splose. No separate consumer cloud file-storage service is used for client clinical records. Speechie Steph applies safeguards proportionate to the sensitivity of health information, including:

- using business-controlled accounts and devices rather than shared household or public accounts;
- strong unique passwords, multi-factor authentication where available, automatic screen locking and restricted user permissions;

- device encryption, supported operating systems, security updates, reputable endpoint protection and secure backups;
- keeping final clinical records in Splose and/or on the secured business computer as appropriate, limiting unnecessary duplicate copies and periodically reviewing local folders;
- checking email addresses, access permissions and file attachments before sending reports or other sensitive information;
- using encrypted portable media only where necessary, and securely deleting redundant or temporary files when no longer required;
- not leaving devices or paper records unattended in vehicles, public locations, schools, homes or shared spaces; and
- ensuring devices are securely erased or professionally destroyed before disposal, resale or reassignment.

Workers and contractors may access information only to the extent required for their role and must comply with confidentiality, privacy and security obligations.

11. Email, SMS, online bookings and telehealth

Speechie Steph uses Microsoft Outlook for business email. Email, SMS and online communications may carry privacy and security risks, including misdirection, interception and access by another person using the recipient's device or account. We use these channels for reasonable clinical and administrative communications and take steps to minimise sensitive information in routine messages.

Clients may request a preferred communication method or ask that particular information not be sent by email or SMS. We may use secure links, password protection, identity checks or another communication method where the information is especially sensitive. Appointment reminders may contain limited identifying information.

Telehealth services are delivered using approved systems and reasonable privacy safeguards. Clients are encouraged to participate from a private location and to tell us who else is present. We do not record telehealth sessions unless this has been specifically explained and agreed, or recording is otherwise authorised by law.

12. Audio, video and AI-assisted documentation

Speechie Steph may use approved digital tools to assist with clinical administration or documentation. We do not make an audio or video recording of a clinical interaction, or use a recording-based transcription feature, without first providing clear information and obtaining specific consent unless collection is required or authorised by law.

Where an approved AI-assisted documentation tool is used, the output is treated as a draft and is reviewed, corrected and approved by a qualified clinician before it is relied on or entered into the clinical record. Speechie Steph remains responsible for clinical decisions and record accuracy.

Identifiable client information must not be entered into public or general-purpose AI tools that have not been approved for clinical use, privacy, security and contractual suitability. Recording or transcription data is retained only for as long as necessary for the stated purpose and in accordance with the applicable provider settings, consent and this policy.

13. Overseas processing and disclosure

Speechie Steph prefers Australian data storage for identifiable clinical information. Splose states that Australian user data is stored in Australia. However, Microsoft Outlook, Stripe, ANZ, Splose service providers and other technology or business providers may process information, provide support or permit authorised access from outside Australia.

The information handled by each provider differs. Microsoft Outlook may process email content and account information. Stripe and ANZ generally process billing, contact and transaction information and are not intentionally provided with clinical reports. Before disclosing personal information to an overseas recipient, we take reasonable steps required by Australian privacy law, having regard to the nature of the information, the recipient, contractual safeguards and the relevant service.

Likely overseas processing locations for current providers may include the United States, Ireland, India, New Zealand, the United Kingdom, Singapore, the Philippines, Canada, Fiji, Israel, Taiwan and member states of the European Union, as well as other countries where a provider or its authorised service providers operate. Provider infrastructure and subprocessors can change over time.

14. Data quality

We take reasonable steps to ensure the personal information we collect, use and disclose is accurate, complete, current and relevant for the purpose. Clients and authorised representatives are encouraged to tell us promptly when contact details, authority, health information, risks, funding arrangements or other relevant information changes.

15. Security safeguards

We take reasonable technical, physical and administrative steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure. Safeguards may include access controls, role-based permissions, confidentiality obligations, secure storage, encryption, multi-factor authentication, backups, secure disposal, software updates, incident response procedures, privacy training and periodic review of systems and risks.

No system can be guaranteed to be completely secure. We continually review safeguards and respond to identified risks, incidents and changes in technology or service delivery.

16. Retention, destruction and de-identification

Speechie Steph retains clinical and business records for the period reasonably required for continuity of care, professional accountability, insurance, funding, tax, legal and regulatory purposes. Unless a longer or different period applies, our general clinical record retention approach is:

- adult client records: at least seven years after the last service or last entry in the record; and
- child client records: at least until the client reaches 25 years of age, or seven years after the last service or last entry, whichever is later.

Certain records, including NDIS incident, complaint, financial or contractual records, may be retained for a different minimum period under applicable rules. Records may also be kept longer

where reasonably required for an unresolved complaint, legal claim, safeguarding matter, insurance requirement or continuity of care.

When information is no longer required and no law, court order or other legitimate obligation requires retention, we take reasonable steps to securely destroy or de-identify it. De-identified information may be retained for service evaluation, quality improvement, education or business analysis where re-identification is not reasonably likely.

17. Accessing and correcting information

An individual may request access to personal information we hold about them and may ask us to correct information they believe is inaccurate, out of date, incomplete, irrelevant or misleading. A parent, guardian, nominee or other person may request access only where they have appropriate authority.

Requests can be made using the contact details in section 23. We may ask for identity and authority verification. We aim to respond within 30 calendar days. We do not charge for making an access or correction request, but may charge a reasonable, non-excessive fee for providing access, such as copying, retrieval or postage costs. We will discuss any likely fee before proceeding.

Access may be refused or limited where permitted by law, including where access would create a serious threat to life, health or safety, unreasonably affect another person's privacy, reveal commercially sensitive evaluative information, prejudice legal proceedings, or be otherwise unlawful. Where possible, we will consider alternatives such as redaction, a summary, supervised access or access through an agreed health professional. If we refuse access or correction, we will provide written reasons where required and explain how to complain.

Clinical records are not usually altered by deleting an original entry. Corrections are made through an appropriately dated amendment, addendum or notation that preserves the integrity of the record.

18. Data breaches

A data breach occurs when personal information is lost or accessed, disclosed, altered or destroyed without authorisation. Suspected breaches are assessed promptly, contained where possible, documented and investigated. We take remedial action to reduce harm and prevent recurrence.

Where a breach is likely to result in serious harm and is an eligible data breach under the Notifiable Data Breaches scheme, we will notify affected individuals and the Office of the Australian Information Commissioner as required. We may also notify other regulators, funding bodies, insurers, technology providers or law enforcement where required or appropriate.

19. Direct marketing

We do not use health information for direct marketing without consent. Where a person has separately agreed to receive newsletters, service updates or other promotional communications, each electronic communication will provide a simple way to unsubscribe. Opting out of marketing does not affect essential clinical, safety, billing or appointment communications.

20. Website, cookies and analytics

Our website may use essential cookies and, if enabled, analytics or embedded third-party services to understand website use, operate booking forms and improve services. These tools may collect technical information such as IP address, device and browser information, pages viewed and referral source. We do not intentionally configure advertising or analytics tools to collect health information from clinical or intake forms.

Website visitors can manage cookies through their browser and any cookie preference tool provided on the website. Third-party websites linked from our website have their own privacy practices, and Speechie Steph is not responsible for those external sites.

21. Privacy complaints

A person who believes Speechie Steph has mishandled their personal information may make a privacy complaint using the contact details in section 23. Please describe the concern, relevant dates, the information involved and the outcome sought. We will acknowledge the complaint, investigate it fairly, protect the complainant from adverse treatment and aim to provide a written response within 30 days. Complex matters may take longer, in which case we will provide an update.

If the complaint is not resolved, the person may contact the Office of the Australian Information Commissioner. Concerns about a health service in Queensland may also be raised with the Office of the Health Ombudsman. Concerns about the quality or safety of NDIS supports or services may be raised with the NDIS Quality and Safeguards Commission.

22. Changes to this policy

We review this policy at least annually and when our services, systems, providers, legal obligations or information-handling practices change. The current version will be available on our website and on request. Material changes will be communicated where appropriate.

23. Contact details

Privacy Officer: Principal Speech Pathologist, Speechie Steph

Email: hello@speechiesteph.com.au

Phone: 0415 270 031

Website: www.speechiesteph.com.au

Last updated: 12 July 2026

Appendix A - Short privacy collection notice for Splose

Use this notice on online booking, referral, intake and consent forms. Add a link to the full Privacy Policy.

Privacy collection notice

Speechie Steph collects personal and health information to respond to your enquiry, determine service suitability, provide speech pathology services, maintain clinical records, communicate with authorised people involved in care, manage appointments, prepare reports, process invoices and funding claims, manage safety and complaints, and meet legal and professional obligations.

We usually collect information from you or your authorised representative. With consent, or where permitted by law, we may also collect or disclose relevant information to referrers, health and education providers, support coordinators, plan managers, the NDIA, insurers and contracted service providers. We use Splose for practice management and secure clinical administration.

You may request access to or correction of your information, change or withdraw consent, or make a privacy complaint. Some information is necessary for us to provide safe services, process funding or meet legal obligations; if it is not provided, we may be unable to provide all or part of the requested service. Our full Privacy Policy explains storage, security, retention, overseas processing and complaint options.

Contact: hello@speechiesteph.com.au | 0415 270 031 | Full policy: www.speechiesteph.com.au or available on request

Appendix B - Consent wording for intake forms

Keep required and optional consents separate. The wording below is a starting point and should be adapted to each form and client.

Required privacy acknowledgement

- I confirm that I have read, or have been offered assistance to understand, the Speechie Steph Privacy Policy and privacy collection notice.
- I consent to Speechie Steph collecting, holding, using and disclosing personal and health information as reasonably necessary to assess and provide services, maintain clinical records, communicate about appointments, manage billing and funding, manage safety and meet legal and professional obligations.
- I understand that I can ask questions, request access or correction, and withdraw or change consent, although this may affect the services Speechie Steph can provide.

Information-sharing authority - complete with names or categories

- I authorise Speechie Steph to exchange relevant information with the following people or organisations for the stated purpose: _____.
- This authority remains in place until the end of service unless I change or withdraw it earlier.

Communication preference

- I agree to receive appointment and service communications by: ☐ email ☐ SMS ☐ phone ☐ secure link ☐ other: _____.
- I understand ordinary email and SMS may carry privacy risks and I can request another method for sensitive information.

Optional recording or AI-assisted transcription consent

- I consent to the specific session or interaction being audio/video recorded or transcribed using the approved tool explained to me, for the purpose described in the relevant consent form.
- I understand whether the recording will be stored, who can access it, the provider used, how long it will be retained, and that I may decline or withdraw consent without affecting access to ordinary services, unless the recording is essential to the agreed service and this has been explained.