



Privacy Policy

Privacy Policy, confidentiality and responsible AI use

How Frankly Speaking Speech Pathology collects, protects, uses and shares personal and health information, including when artificial intelligence and generative AI are used.

CLIENT RIGHTS AT A GLANCE

You may ask what information we hold, request access or correction, ask how AI was used, refuse or withdraw consent to client-specific AI use, and make a privacy complaint. Refusing client-specific AI use will not prevent access to clinically appropriate speech pathology services.

1. About this policy

Frankly Speaking Speech Pathology is committed to protecting the privacy, dignity and confidentiality of clients, families and other people whose information we hold.

This policy explains the kinds of personal and health information we collect, how and why we collect it, how we store and disclose it, how artificial intelligence and generative artificial intelligence may be used, and how a person may access or correct information or make a complaint.

In this policy, “the Practice”, “we”, “us” and “our” mean Frankly Speaking Speech Pathology. “Client” includes a current, former or prospective client and, where relevant, their parent, guardian, carer, nominee, support person or authorised representative.

This policy applies to information handled through mobile, school, preschool, home, telepractice, telephone, online and administrative activities. It should be read with the Practice’s consent forms, service agreement, fee schedule, complaints information, data-breach procedure and separate AI consent documentation where applicable.

What this policy does not do

Agreeing to this Privacy Policy does not, by itself, provide consent for every possible use of AI, audio or video recording, research, marketing or disclosure to another person. Separate consent will be sought where the proposed activity requires it.

2. Legal, ethical and professional framework

Frankly Speaking Speech Pathology manages personal and health information under applicable Commonwealth and New South Wales privacy requirements, including:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs);
- Health Records and Information Privacy Act 2002 (NSW) and the 15 Health Privacy Principles (HPPs);
- the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act 1988;
- Health Records and Information Privacy Regulation 2022 (NSW), where applicable;
- child-protection, court, funding, taxation, health, safety and record-keeping laws that authorise or require information handling; and other privacy, confidentiality and information-security requirements that apply to the Practice’s activities.

SPEECH PATHOLOGY AUSTRALIA AND PROFESSIONAL OBLIGATIONS

The Principal Speech Pathologist also practises in accordance with applicable professional standards and guidance issued by Speech Pathology Australia, including:

- Speech Pathology Australia Code of Ethics 2020;
- Professional Standards for Speech Pathologists in Australia 2020;
- Speech Pathology Scope of Practice in Australia 2022;
- Artificial Intelligence in Speech Pathology: Ethical Considerations - Position Statement;
- Ethical Considerations When Using Artificial Intelligence in Speech Pathology: FAQs for SPA Members;
- Speech Pathology Australia guidance concerning informed consent, confidentiality, health records, documentation, complaints and data breaches; and
- other current Speech Pathology Australia policies, position statements, practice guidance and professional resources relevant to the service provided.

These professional obligations guide how the Practice obtains consent, respects autonomy, provides accessible information, protects confidentiality, keeps accurate records, uses evidence, recognises cultural and linguistic diversity, works within competence and scope of practice, and remains accountable for all clinical decisions and documents.

The Practice also has regard to the National Code of Conduct for Health Care Workers as applied in NSW, including requirements to provide safe, ethical and competent health services and to obtain appropriate consent.

Professional accountability does not transfer to technology

A software provider, AI tool, template or automated suggestion does not take responsibility for the service. The Principal Speech Pathologist remains responsible for professional judgement, accuracy, safety, privacy, communication and the final content of every document issued by the Practice.

3. Information we collect

We collect personal information and sensitive health information that is reasonably necessary to assess a referral, provide speech pathology services and operate the Practice. Depending on the person and service, this may include:

- names, preferred names, dates of birth, pronouns, addresses and contact details;
- details of parents, guardians, carers, nominees, emergency contacts and authorised representatives;
- information about parental responsibility, court orders, consent authority or restrictions on information sharing;
- Medicare, private health insurance, NDIS and other funding or claiming information;
- invoicing, payment and transaction information;
- referral information and the reason services are requested;
- developmental, medical, disability, health, medication, allergy, hearing, vision, feeding and family history;
- pregnancy, birth and newborn information where relevant to the referral;
- speech, language, literacy, fluency, voice, social communication, oral-motor and participation information;
- assessment responses, scores, observations, therapy goals, progress and clinical reasoning;
- education, preschool or school information, attendance, adjustments, learning supports and reports;
- family, cultural, linguistic, social and communication information relevant to safe, responsive care;
- information provided by health, disability and education professionals;
- clinical notes, reports, letters, plans, emails and other correspondence;
- audio, video, photographs or work samples where separate consent has been obtained;
- appointment, attendance, communication, complaints, incidents and feedback records; and

- other information reasonably required to provide safe, ethical and appropriate services.

We will not collect sensitive information merely because it may be convenient. Sensitive information will be collected with consent or where collection is otherwise authorised or required by law. We aim to collect the minimum information reasonably necessary for the relevant purpose.

CHILDREN, YOUNG PEOPLE AND LEGAL AUTHORITY

Most clients of the Practice are children or young people. We will consider the client's age, capacity, communication needs, circumstances and legal arrangements when deciding who may give consent, receive information, request access or make decisions about disclosure. We may ask for evidence of parental responsibility, guardianship, nomination, authority or relevant court orders.

Where appropriate, the child or young person will be given an accessible explanation and supported to express their views or assent. Information will not automatically be provided to every family member merely because they are related to the client.

4. How we collect information

We may collect information:

- directly from the client, parent, guardian, carer, nominee or authorised representative;
- through enquiry, intake, consent, case-history, previous assessment reports and questionnaire forms;
- during telephone, SMS, email, video or face-to-face communication;
- during assessment, therapy, consultation, observation or review;
- through the Practice's booking, practice-management, payment, telepractice and online-form systems;
- from a referrer or another health, disability, education or support professional, with consent or lawful authority;
- from a school, preschool or other service attended by the client, with consent or lawful authority;
- from Medicare, the NDIS, private health insurers or another funding body where relevant;
- through reports, assessments, plans, recordings or other documents provided to us; and
- where collection is required or authorised by law.

Where practicable, information will be collected directly from the person concerned or their authorised representative. When information is collected from someone else, we will take reasonable steps to make the person aware of the collection where required and appropriate.

A person who gives us information about another individual should have authority to do so and should avoid providing information that is unnecessary for the stated purpose.

5. Why we collect, use and hold information

Information may be collected, used and held to:

- respond to enquiries and determine whether the Practice can safely and appropriately provide a service;
- arrange, confirm and manage appointments;
- provide person-centred, culturally responsive and evidence-informed assessment, intervention, consultation and review;
- develop goals, clinical plans, recommendations, resources and home-practice activities;
- prepare and maintain accurate clinical notes, reports, letters and service records;
- communicate with clients, families and authorised members of the support team;
- coordinate care with health, disability and education professionals;
- process Medicare, private health insurance, NDIS and other funding or claiming arrangements;
- issue invoices, process payments and manage accounts;
- meet Speech Pathology Australia ethical, professional and documentation expectations;
- undertake supervision, consultation, reflective practice, audit and quality improvement using appropriately protected information;
- manage complaints, incidents, insurance, risk, legal matters and practice continuity;
- comply with legal obligations and protect the health, safety or welfare of a person; and
- administer, secure and improve the Practice.

Where we propose to use information for a purpose that is not the primary purpose of collection or a directly related purpose that a person would reasonably expect, we will seek consent unless another use is authorised or required by law.

6. Consent, choice and accessible communication

Consent is an ongoing process, not a one-time signature. We will provide enough information for a person to understand the proposed collection, use or disclosure and make a voluntary decision. The information provided will be proportionate to the activity and its risks.

Consistent with the Speech Pathology Australia Code of Ethics, consent processes will respect autonomy, dignity, communication needs, culture, language and the person's right to ask questions. Information may be provided using plain language, visual supports, an interpreter, supported decision-making, repetition, additional processing time or another accessible format.

Consent may be withdrawn for future activities, subject to legal requirements and practical limits. Withdrawal does not require the Practice to destroy health records that must be retained by law, undo disclosures already lawfully made, or remove information from a third-party system where deletion is not technically or legally available. We will explain any relevant limitation.

CONSENT FOR INFORMATION SHARING

Consent to receive speech pathology services does not automatically authorise disclosure to every school, professional, family member, software provider or AI system. The Practice will document the people or organisations authorised to receive information and any limits on the authority.

REFUSING AI USE

A client or authorised representative may refuse or withdraw consent to client-specific AI use. Refusal will not be used as a reason to refuse speech pathology services. The Practice will use a reasonable non-AI alternative, although the alternative process may take longer where manual drafting, transcription or administration is required.

7. How information may be used and disclosed

The Practice may use or disclose relevant information to:

- the client and an authorised parent, guardian, nominee or representative;
- a referring practitioner;
- health professionals involved in the client's care;
- schools, preschools, teachers and learning-support staff;
- NDIS providers, support coordinators or other disability supports;
- Medicare, private health insurers and funding bodies;
- accountants, insurers, auditors, legal advisers and other professional advisers;
- practice-management, payment, cloud-storage, email, security, telepractice and IT providers;
- approved AI or software providers where permitted under this policy and the applicable consent arrangements;
- courts, tribunals, regulators, police, child-protection bodies or government agencies where required or authorised by law; and
- another person where necessary to lessen or prevent a serious threat to health or safety and disclosure is legally permitted.

Only information reasonably necessary for the relevant purpose will be disclosed. Consent to communicate with a person or organisation does not automatically constitute consent to disclose information to an AI provider.

The Practice does not sell or rent client information.

INFORMATION REQUIRED BY LAW

Privacy and confidentiality may be limited where disclosure is required or authorised by law. This may include a subpoena or court order, mandatory reporting, child-protection information exchange, a serious threat to health or safety, or an investigation by an authorised body. Where lawful and safe, the Practice will explain the disclosure and record what information was shared and why.

8. Artificial intelligence and generative AI

Frankly Speaking Speech Pathology may use artificial intelligence (AI) and generative artificial intelligence (GenAI) tools, including general-purpose AI assistants, AI features embedded within Microsoft and other business software, research assistants, writing and readability tools, design tools, transcription or clinical-documentation tools, and AI functions contained within practice-management or telehealth platforms. Examples may include ChatGPT, Microsoft Copilot, Anara, Hemingway Editor, Grammarly, Canva, Adobe Acrobat AI Assistant and other tools assessed by the Practice from time to time. The use of these tools is to support selected business, administrative, research and clinical-documentation tasks. AI is a supporting tool only. It does not replace the Principal Speech Pathologist's professional knowledge, clinical reasoning, ethical judgement, relationship with the client or accountability.

Examples of tools that may be used include:

- ChatGPT;
- Anara;
- Hemmingway Editor;
- Microsoft Copilot and AI-assisted features within Microsoft Word, Outlook, PowerPoint, Excel, OneNote, Teams and other Microsoft software;
- AI-assisted functions within practice-management, telepractice, transcription, research, accessibility, design, security, cloud and productivity applications; and
- other AI-enabled systems that are assessed and approved for a clearly defined purpose.

The particular tools used may change as technology, privacy protections, evidence and professional guidance develop. A new tool will not be used with client information merely because it has been added automatically to an existing software product.

8.1 PERMITTED PURPOSES

Subject to the safeguards below, AI may assist with:

- general business policies, procedures, templates and administrative material;
- formatting, spelling, grammar, readability and plain-language editing;
- draft structures for letters, reports, resources and correspondence;
- general, non-client-specific educational or therapy activity ideas;
- organising and summarising published research or public information;
- searching professional literature and identifying themes for clinician review;
- preparing general website, social-media or practice information;
- document consistency checks and productivity functions; and
- client-specific drafting, summarising or transcription only when the additional requirements in this section are met.

8.2 DEFAULT INFORMATION RULE

No direct identifiers in publicly available AI tools

As a default rule, the Practice will not enter directly identifying client information or sensitive health information into a publicly available or general consumer AI tool. A provider's convenient interface or confident output does not make the product suitable for health information.

Information that **will not** be entered into general consumer AI tools includes:

- client names, identifying initials, dates of birth, addresses, telephone numbers or email addresses;
- Medicare, NDIS, health-fund, payment or other identifying numbers;
- identifiable photographs, audio or video;
- school, preschool, service-provider or location details that could identify the client;
- complete identifiable reports, assessment records or correspondence; and
- combinations of age, diagnosis, family circumstances, location, school, unusual presentation or other details that could reasonably permit re-identification.

8.3 TOOL-SPECIFIC PRACTICE RULES

Tool or feature	Typical Practice use	Client-information rule
ChatGPT	General drafting, editing, templates, plain-language material, brainstorming and research support. Client-specific drafting may occur only under the safeguards in this section.	No direct identifiers in publicly available or general consumer accounts. Use the minimum necessary information. Client-specific use requires documented informed consent and clinician review.
Hemingway Editor	Reviewing readability, sentence complexity, grammar, passive voice and writing style; simplifying text; adjusting tone; and supporting the preparation of clear, plain-language client resources, correspondence and general practice documents. Hemingway Editor Plus includes AI-assisted rewriting, document review and editing features.	Used for published, public, synthetic or appropriately non-identifiable material. Identifiable health information will not ordinarily be entered.
Anara	Reading, organising and summarising published research, public sources and professional literature to support report writing where evidence is required.	Used for published, public, synthetic or appropriately non-identifiable material. Identifiable health information will not ordinarily be entered.
Microsoft AI features	Productivity assistance within approved Microsoft software, including drafting, summarising, formatting and administrative functions.	Use only within Practice-approved accounts and settings. Client information will be used only after the feature, data flow, retention and account protections have been reviewed and the required consent obtained.
Other embedded AI	Functions within practice-management, telepractice, transcription, accessibility, security, design or cloud applications.	The feature must be identified, assessed and approved. Automatic availability does not amount to approval. High-risk or client-specific use requires a privacy assessment and informed consent.

8.4 CLIENT-SPECIFIC AI USE AND INFORMED CONSENT

Where AI use is client-specific, involves identifiable or potentially re-identifiable information, contributes directly to a clinical record, or involves recording or transcription, the Practice will:

- define the proposed purpose and consider whether AI is necessary and proportionate;
- assess whether the product is suitable for health information and review privacy, security, retention, deletion, access, subprocessors, model-training and overseas-processing arrangements;
- explain the name and nature of the tool and how it will and will not be used;
- explain what information will be entered, uploaded, recorded or processed;
- explain whether information will be identifiable, coded or de-identified and the remaining re-identification risk;
- explain known benefits, limitations and material risks, including accuracy, bias and confidentiality risks;
- explain whether the output will form part of the client record;

- explain who may access the information and any known storage or processing location;
- identify an available non-AI alternative;
- obtain voluntary, specific, current and documented informed consent before proceeding, unless the use is otherwise authorised or required by law; and
- seek renewed consent if the tool, purpose, information or material risk changes.

Consent for client-specific AI use will be separate from general consent to receive services. It will not be inferred merely because a person accepted this policy, completed an intake form or agreed to ordinary clinical software.

8.5 AUDIO, VIDEO, TRANSCRIPTION AND MEETING SUMMARIES

AI-enabled recording, transcription, dictation or meeting-summary functions will not be used during a client interaction unless the Practice has confirmed that the product is suitable and has obtained the required audio, video and AI consent. The person will be told what is recorded, why, where it is processed, how long it is retained and whether a recording or transcript becomes part of the health record.

8.6 HUMAN REVIEW AND PROFESSIONAL ACCOUNTABILITY

The Principal Speech Pathologist remains accountable for information generated wholly or partly with AI. Before AI-assisted content is relied upon, recorded, communicated or published, it will be reviewed as appropriate for:

- factual and clinical accuracy;
- fabricated, incomplete, misleading or outdated information;
- the quality and authenticity of cited sources;
- evidence base and limits of the evidence;
- bias, stereotyping and unfair assumptions;
- cultural and linguistic responsiveness and safety;
- neurodiversity-affirming, respectful and accessible language;
- relevance to the individual client and their participation goals;
- privacy, confidentiality and data minimisation;
- copyright, intellectual property and assessment-material licensing; and
- consistency with the Code of Ethics, Professional Standards and scope of practice.

AI-generated references, quotations, scores or clinical claims will not be accepted as genuine without verification. Copyrighted assessment manuals, test items, record forms or proprietary materials will not be uploaded to an AI system unless the licence and product arrangements clearly permit that use.

8.7 DECISIONS AI WILL NOT MAKE ON ITS OWN

AI will not be the sole basis for:

- diagnosing a communication or swallowing condition;
- interpreting a standardised assessment or determining assessment validity;
- deciding whether a person is accepted, discharged or refused a service;
- setting therapy frequency, goals or recommendations;
- determining eligibility for funding, education support or another service;
- making child-safety, mandatory-reporting, clinical-risk or emergency decisions; or
- another decision that has a significant effect on a client's rights, welfare or access to support.

8.8 AI RECORDS AND TRANSPARENCY

When AI materially contributes to a client-specific document or process, the final clinical record will contain enough information to support professional accountability. Depending on the circumstances, this may include the purpose, tool, consent, nature of information processed, clinician review and significant corrections made.

The final clinician-approved document may form part of the health record. Unverified AI output will not be retained as though it were an approved clinical finding. A client or authorised representative may ask whether AI materially contributed to a specific clinical document.

9. Third-party technology providers

The Practice relies on third-party services to operate. These may include practice-management, online-form, appointment-reminder, telepractice, payment, email, document, cloud-storage, backup, accounting, cybersecurity, research and AI services.

Before using a provider to handle client information, the Practice will take reasonable steps to consider:

- the sensitivity and amount of information involved;
- whether the provider is designed and contractually suitable for health information;
- access controls, authentication, encryption and audit capability;
- data location, subprocessors and overseas processing;
- retention, deletion, export and account-closure arrangements;
- whether information may be used for model training, product development, advertising or another secondary purpose;
- data-breach notification and response arrangements;
- the ability to support access and correction requests; and
- whether a privacy impact assessment or additional consent is required.

Third-party providers have their own terms and privacy practices. The Practice will not represent that a provider is risk-free. We will choose and configure services with regard to our legal and professional obligations and will review material changes where practicable.

Payment-card details may be collected and stored by an authorised payment provider. The Practice will not have access to the full card number.

10. Overseas disclosure and processing

Some cloud, software, support and AI providers may store or process information outside Australia or permit access from another country. The relevant country or region depends on the provider, account type, infrastructure and subprocessors in use.

Before identifiable personal or health information is disclosed to an overseas recipient, the Practice will consider whether the disclosure is lawful and appropriate and will take the reasonable steps required by the APPs and HPPs. Where practicable, likely countries or regions will be identified in this policy, a collection notice, consent form or service-specific explanation.

Because provider infrastructure can change, exact locations will be reviewed periodically. Where a location is not confirmed, the Practice will not guess. Client-specific AI consent will include the available information about overseas processing and any material uncertainty.

11. Storage and security

Information may be stored electronically and, where necessary, in hard copy. The Practice uses reasonable safeguards appropriate to the sensitivity of health information. Measures may include:

- password-protected devices and accounts;
- multi-factor authentication;
- device encryption and secure screen locking;
- secure cloud systems and backups;
- restricted access and separate business accounts;
- current software, security updates and threat protection;
- secure transmission methods where available;
- locked storage for paper records;
- data minimisation and de-identification;
- privacy settings that limit model training or secondary use where available;
- periodic review of third-party provider and AI settings; and
- secure destruction or disposal when information is no longer required.

No electronic system is completely free from risk. The Practice will review safeguards in light of the sensitivity of the information, changes in technology, provider changes, incidents, complaints and updated legal or professional guidance.

The fact that AI functionality is activated or available within software does not itself authorise the Practice to use that feature with client information.

12. Clinical records, retention and secure disposal

Clinical and administrative records will be current, accurate and sufficiently complete to explain the service provided, information relied upon, clinical reasoning, consent, significant communication and decisions. This reflects both legal record-keeping duties and Speech Pathology Australia's Code of Ethics and Professional Standards.

Under NSW health-privacy requirements, the Practice will generally retain:

- health information collected about an adult for at least 7 years from the last occasion on which a health service was provided; and
- health information collected while the client was under 18 until the client reaches 25 years of age.

Records may be retained longer where reasonably required for legal, insurance, complaint, safeguarding, funding, continuity-of-care or professional reasons.

When information is no longer required and there is no lawful reason to retain it, the Practice will take reasonable steps to securely destroy or permanently de-identify it. Where required, a record of destruction, transfer or disposal will be maintained.

If the Practice closes, sells or transfers the business, records will be managed in accordance with applicable law and reasonable steps will be taken to support continuity, secure custody and client notification where required.

13. Access and correction

A person may request access to personal or health information that the Practice holds about them. Requests should identify the information sought and the preferred form of access. The Practice may ask for evidence of identity and authority before releasing information.

The Practice will process requests as quickly as reasonably possible. A private NSW health service provider must provide a formal response to an access request within 45 calendar days. Where the APPs require a shorter reasonable period, the Practice will aim to respond within that period.

Access may be provided by electronic or paper copy, inspection, explanation, summary or another reasonable form. A reasonable fee may be charged for the cost of retrieving, reviewing, copying or providing access, but no fee will be charged merely for making the request. A fee will not be excessive or used as a barrier to continuity of care.

Access may be refused or limited where permitted by law, including where disclosure would pose a serious threat to health or safety, unreasonably affect another person's privacy, relate to certain legal proceedings, reveal evaluative information in a commercially sensitive decision process, or otherwise fall within a lawful exception. Where access is refused, the Practice will provide a written explanation and complaint options, subject to law.

A person may ask the Practice to correct information that is inaccurate, incomplete, out of date, irrelevant or misleading. If the Practice does not agree to make the requested amendment, the person may ask for a statement of the requested correction to be attached to the record where required by law.

14. Website, email, SMS and social media

WEBSITE AND ONLINE FORMS

When the Practice operates a website, booking page or online form, the service provider may automatically record technical information such as IP address, device and browser type, date and time of access, pages viewed, referring site, cookies and security logs. This information may be used to operate, secure and improve the service.

Information submitted through a website, online form or booking system will be handled under this policy. The Practice will not ask a person to submit detailed clinical information through a public contact form where a more secure method is available.

COOKIES AND ANALYTICS

A website may use essential cookies or analytics tools. The particular cookies and providers will be described in the website notice where required. Browser settings may allow cookies to be limited, although this can affect website functionality.

EMAIL AND SMS

Email and SMS may be used for routine administrative communication, appointment reminders and agreed clinical communication. These methods carry privacy risks, including misdirection, interception or access by another person using the device or account. Highly sensitive documents will be sent using a more secure method where reasonably available.

SOCIAL MEDIA

Social media is not used for confidential clinical communication or urgent support. Messages sent through a social-media platform are also subject to that platform's privacy practices. The Practice will move clinical or identifying communication to an appropriate channel.

EXTERNAL LINKS

The Practice may link to external websites or resources. Unrelated external sites are governed by their own privacy practices. A link does not amount to responsibility for the external site's handling of information.

15. Direct marketing

The Practice may provide information about relevant Practice services where consent has been given or the communication is otherwise permitted by law. Sensitive health information will not be used for direct marketing without appropriate consent.

Marketing communication will provide a reasonable way to opt out. A request to stop marketing will be actioned as soon as practicable. Appointment reminders, invoices, service notices, clinical communication and legal notices are not marketing.

16. Data breaches and security incidents

A data breach may occur when personal information is lost, accessed, disclosed, altered or used without authorisation. A breach may involve the Practice, a device, an email, a paper record, a software provider, an AI provider or another third party.

When a suspected breach occurs, the Practice will:

1. take immediate steps to contain the incident and reduce potential harm;
2. identify what happened, the information involved and the people who may be affected;
3. contact relevant technology providers, insurers, advisers or authorities where necessary;
4. undertake a reasonable and expeditious assessment and take reasonable steps to complete any required eligible-data-breach assessment within 30 days;
5. consider remedial action, including account security, deletion, recovery, correction or changed service arrangements;
6. document the incident, decisions and actions taken;
7. notify affected people and the Office of the Australian Information Commissioner where the Notifiable Data Breaches scheme requires notification; and
8. consider whether the incident also raises a Speech Pathology Australia ethical concern, clinical-record issue, complaint, child-safety issue or need for quality improvement.

Where a breach involves AI or another software provider, the Practice will also consider whether the information was used outside the authorised purpose, whether consent was adequate, whether information may have been used for training or secondary purposes, and whether future use of the product should be suspended or changed.

17. Privacy concerns and complaints

A person may raise a concern about collection, consent, confidentiality, access, correction, disclosure, security, record keeping, overseas processing, AI use, the accuracy of AI-assisted information or another privacy matter. A concern may be raised even where no reportable data breach has occurred.

Complaints should include, where possible, the person's name and contact details, a description of the concern, relevant dates or events, the outcome sought and any supporting information.

The Practice will:

- acknowledge the complaint;
- consider immediate safety, privacy or service risks;
- investigate fairly, respectfully and confidentially;
- seek further information or independent advice where needed;
- provide updates where the matter cannot be resolved promptly;
- provide a written response within a reasonable period, ordinarily within 30 calendar days; and
- explain any available external review or complaint options.

Making a complaint will not disadvantage a person's access to clinically appropriate services. Where the complaint concerns AI, the Practice may pause the relevant use while the concern is assessed.

EXTERNAL COMPLAINT OPTIONS

Depending on the issue, a person may contact:

- the Office of the Australian Information Commissioner for a complaint under the Privacy Act;
- the Information and Privacy Commission NSW / NSW Privacy Commissioner for a complaint concerning the HRIP Act;
- the NSW Health Care Complaints Commission for a complaint about a health service or unregistered health practitioner; and
- Speech Pathology Australia where the concern relates to the conduct of a Speech Pathology Australia member and the Code of Ethics.

18. Changes to this policy

The Practice may update this policy when laws, professional guidance, services, technology, providers, AI systems or information-handling practices change. The current version will display its effective date and will be made available free of charge.

Material changes to client-specific AI use will be communicated before the changed use occurs. New consent will be sought where the tool, purpose, information or risk changes in a way that makes existing consent insufficient.

The Practice will review this policy at least annually and earlier following a significant incident, complaint, data breach, legal or professional update, new software or AI system, or identified implementation gap.