POLICY

Confidentiality Policy

The Lifestory Practice

Effective date: 30 August 2026 | **Policy contact:** Carrie Gibbons, Practice Manager

Purpose and scope

This policy explains how The Lifestory Practice protects confidentiality in therapy, assessment, support, administration, supervision and related services, and the circumstances in which information may be used or disclosed. It applies to directors, employees, contractors, students and volunteers.

Our confidentiality commitment

Information obtained in the course of providing services is treated as confidential and accessed only for a legitimate work purpose. Information will not be disclosed outside the practice without valid consent unless the disclosure is otherwise required or authorised by law.

Clients are told about confidentiality and its limits before or at the start of services, in a form they can understand. Confidentiality is discussed again when the service, information-sharing arrangements or relevant risks change.

Permitted use within the practice

Relevant information may be accessed by the treating practitioner and authorised administrative or clinical personnel where reasonably necessary to arrange, bill, supervise, provide or review services, manage safety, respond to a complaint or meet legal obligations. Access is role-based and limited to the minimum information needed.

Where more than one practitioner is involved, the client will be informed about the team or shared-care arrangement. Information is not made generally available to all workers merely because they work at the practice.

Consent-based information sharing

Before information is shared with an external person or organisation by consent, the client or authorised decision-maker will be informed of:

- who will receive the information
- the purpose of disclosure
- the type and scope of information
- how long the consent applies
- the right to limit or withdraw consent before disclosure, and any likely consequences.

Consent and any limits are documented. Withdrawal cannot reverse a disclosure already made lawfully. Reports and letters will contain only information reasonably relevant to the agreed purpose.

Limits of confidentiality

Information may be used or disclosed without consent in the following circumstances.

Required or authorised by law

- a valid court or tribunal order, subpoena, warrant or other lawful requirement
- mandatory reporting of a reasonable suspicion that a child or young person is, or may be, at risk of harm, where the duty applies
- reportable-incident or safeguarding duties applying to NDIS, aged-care or other regulated services
- mandatory notifications or disclosures required by applicable professional, public-health or other legislation.

A subpoena does not automatically authorise unrestricted disclosure. The practice will verify the request, obtain legal or professional advice where appropriate, notify the client where lawful and safe, and disclose only what is required.

Serious threat to life, health or safety

Where it is unreasonable or impracticable to obtain consent, information may be used or disclosed if the practitioner reasonably believes this is necessary to lessen or prevent a serious threat to the life, health or safety of any person, or to public health or safety. The belief and disclosure must have a reasonable basis and will be documented.

Other lawful exceptions

Information may also be used or disclosed under another exception in the Privacy Act 1988 (Cth) or other applicable law, including certain enforcement-related situations. The Practice Manager should be consulted before a non-routine disclosure unless delay would create immediate danger or breach a legal deadline.

Minimum necessary disclosure

When disclosure without consent is required or authorised, the practice will share only information reasonably necessary for the purpose, with an appropriate recipient and by a secure method. The client will be informed where lawful, safe and appropriate.

Children, young people and representatives

The practitioner will consider the child or young person's age, maturity, understanding, capacity and applicable law when determining who may consent to information sharing and access records. A young person capable of consenting may have confidentiality rights independent of a parent or guardian.

Parents, guardians, nominees, substitute decision-makers and support people receive information only within their lawful authority and the consent given. Being an emergency contact or paying for services does not, by itself, create unrestricted access to clinical information.

Supervision and professional consultation

Practitioners may discuss clinical work in supervision or professional consultation for quality and safety. Information will be de-identified wherever practicable. If identifiable information is necessary, sharing must have a lawful basis, be limited to what is needed, and occur with a supervisor or consultant who is bound by confidentiality. Clients are informed that supervision forms part of professional practice.

Audio, video and image recording

No clinical session will be audio-recorded, video-recorded or photographed without specific, informed and documented consent from the client or authorised decision-maker and, where appropriate, the client's assent.

Before consent is obtained, the practice will explain:

- the recording type, purpose and people who may access it
- whether recording is optional and that refusal will not disadvantage the client

- how it will be made, transmitted, stored and protected
- the retention period and planned deletion method
- whether separate consent is required for supervision, education, training, research, publicity or another secondary purpose.

Recording consent is documented on a separate consent form or equivalent record; this policy is not itself a recording-consent form. Consent may be withdrawn for future recording and use. A request to delete an existing recording will be considered subject to legal, professional, insurance, funding and record-keeping requirements.

Communication and remote services

The practice uses reasonable safeguards for telephone, email, SMS, telehealth and other electronic communication. Clients are informed that ordinary electronic communication may carry privacy risks. Before leaving detailed voicemail or sending sensitive information, staff will follow the client's recorded communication preferences where practicable.

For telehealth, both practitioner and client should use a private setting where practicable. The practitioner will confirm identity, location and emergency arrangements when clinically relevant and will respond if privacy cannot be maintained.

Storage, access and security

- Paper records are kept in secure areas with controlled access.
- Electronic records are protected through appropriate access controls, authentication, device security, backup and secure systems.
- Staff must not access records out of curiosity, for personal reasons or beyond their role.
- Confidential information must not be discussed where it may be overheard or displayed where unauthorised people may see it.
- Suspected loss, misdirection, unauthorised access or disclosure must be reported immediately to the Practice Manager and managed under the privacy-breach process.

Retention and secure destruction

As a practice standard, clinical records are generally retained for at least seven years after the last service. Records created when a client was under 18 are generally retained until at least the client's 25th birthday. A longer period applies where required by law, professional standards, funding rules, contract, insurance, litigation hold or another legitimate need.

When information is no longer required, it is securely destroyed or permanently de-identified. Destruction is suspended where a complaint, claim, investigation, subpoena, audit or other preservation requirement is current or reasonably anticipated.

Access and correction

Clients may request access to, or correction of, their personal information. Requests are managed under the Privacy Policy. Access may be refused or provided through an appropriate intermediary only where an exception permitted by law applies, such as a serious threat to a person's life, health or safety or an unreasonable impact on another person's privacy. Reasons and review options will be provided where required.

Breaches of confidentiality

Any suspected breach must be reported immediately to the Practice Manager. The practice will contain the breach, assess risk, preserve evidence, notify affected people and regulators where required, document the

response and implement corrective action. Deliberate or reckless breaches may result in disciplinary or contractual action and referral to a regulator or police.

Contact details

Organisation: The Lifestory Practice
ABN: 14 697 722 991
Address: 1A Old Coach Road, Aldinga SA 5173
Primary contact: Carrie Gibbons, Practice Manager
Practice Manager email: Carrie@thelifestorypractice.com.au
General email: admin@thelifestorypractice.com.au
Phone: (08) 7083 8777
Mobile: 0413 006 336
Website: www.thelifestorypractice.com.au

Policy references

- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Office of the Australian Information Commissioner, Guide to Health Privacy
- Children and Young People (Safety) Act 2017 (SA) and current Department for Child Protection guidance
- Applicable NDIS, aged-care and professional confidentiality requirements
- The Lifestory Practice Privacy, Informed Consent, Incident Management and Information Sharing policies.