SOUTHSIDE
Montessori School

Privacy Policy

1. Introduction

Southside Montessori School, operated by Southside Montessori Society (ABN 39 001 686 344), (the School, we, us) is committed to protecting the privacy of students, parents/guardians, staff, contractors, volunteers and members of our community.

This Privacy Policy explains how we collect, hold, use and disclose personal information, and how you can access or correct your information or make a privacy complaint. This is intended to meet the requirements of the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Because we are located in New South Wales, we are also bound by the Health Records and Information Privacy Act 2002 (NSW) in relation to health information, and we handle such information in accordance with the Health Privacy Principles under that Act.

Under the Privacy Act 1988 (Cth), the Australian Privacy Principles do not apply to certain acts and practices directly related to employee records of current or former employees. As a result, this Privacy Policy does not apply to the School's handling of employee records where this exemption applies.

However, this exemption does not apply in all circumstances. In particular, health information about staff may also be subject to the Health Records and Information Privacy Act 2002 (NSW). The School handles such information in accordance with applicable legal obligations.

This includes circumstances where information is collected before employment commences (such as during recruitment), or where information relates to contractors or volunteers, to whom the employee records exemption does not apply.

Privacy at a glance

This summary provides a high-level overview of how we handle personal information. It should be read together with the full Privacy Policy.

- We collect personal information that is reasonably necessary to provide education, care, and related services.
- This includes information about students, parents/guardians, staff, contractors, and volunteers, and may include sensitive information such as health information.
- We usually collect information directly from you, but may also collect it from authorised representatives or relevant third parties where appropriate.
- We use and disclose personal information to support education, student wellbeing, school operations, and to comply with legal obligations.
- Some of the service providers we use may store or process personal information overseas (for example, in the United States or European Union).
- We take reasonable steps to protect personal information and to ensure it is handled securely.

- You have the right to access and request correction of your personal information.
- You can contact us or make a privacy complaint at any time using the details in this policy.

For more detail about any of these matters, please read the full Privacy Policy below.

2. What information we collect and hold

The types of information we may collect and hold depend on our relationship with you (student, parent, staff member, etc.) and what is reasonably necessary for our functions and activities. We may collect personal information, including health and other sensitive information. This includes health information, which is also regulated under NSW health privacy laws as described in Section 1.

Where we collect sensitive information (including health information), we will generally do so with consent, unless an exception under applicable law applies.

Health information is handled in accordance with the Health Privacy Principles under the Health Records and Information Privacy Act 2002 (NSW). We primarily collect and use health information to support student wellbeing, provide appropriate care, and meet our duty of care and legal obligations.

(a) Students and parents/guardians

Examples may include:

- name and contact details; family/parent contact details; emergency contacts
- date of birth, gender, language background, previous school, and religion
- learning and assessment information (e.g. academic reports, attendance and wellbeing/behaviour records, results of tests/examinations)
- conduct and complaint records or other behaviour notes
- health information required for duty of care (e.g., details of disabilities and/or allergies, dietary requirements, absence notes, immunisation details, medical reports and plans, name of doctor, incident reports)
- information about referrals to government agencies
- health fund details and Medicare number
- photos & videos including at school events
- school surveillance information
- parent education, occupation, language spoken at home, nationality, country of birth, visa/residency status
- authorised pick-up contacts
- communications with the School
- billing/fee information where applicable
- court orders and related legal documents
- volunteering information

(b) Staff, contractors, and volunteers

Examples may include:

- name and contact details (including next of kin); date of birth; religion
- qualifications; employment history; professional development history
- Working With Children / child safety related information where required
- criminal records
- payroll and banking details, including superannuation details

- health information (e.g. details of disability and/or allergies; medical certificates)
- complaint records and investigation reports
- incident and workplace health/safety information where relevant
- leave details
- photos and videos at school events
- workplace surveillance information
- work emails and private emails and internet browsing history

3. How we collect information

We collect information in a number of ways, including:

- directly from you (enrolment forms, medical forms, interviews, emails, phone calls, meetings)
- from your authorised representatives (e.g., parent/guardian, or a treating professional with consent)
- from third parties where reasonably necessary (e.g., previous schools, referees for staff applicants)
- through school systems and devices that were used for school purposes (e.g., login logs, device management, student email monitoring)
- through CCTV and other safety or security measures, and through monitoring of school ICT systems that were used for school purposes, in accordance with applicable laws (including the Workplace Surveillance Act 2005 (NSW)) and with appropriate notice where required.

Where workplace surveillance applies to staff, the School complies with the Workplace Surveillance Act 2005 (NSW), including providing notice of surveillance and implementing appropriate policies.

We aim to collect information directly from the individual where reasonable and practicable, and only collect what is reasonably necessary.

At or before the time we collect personal information (or as soon as practicable afterwards), we take reasonable steps to provide individuals with a collection notice. This notice will include details such as:

- the identity and contact details of the School;
- the purpose for which the information is collected;
- the main consequences (if any) of not providing the information;
- the types of organisations to which we usually disclose the information;
- whether the information is likely to be disclosed overseas;
- how to access and correct personal information; and
- how to make a privacy complaint.

This Privacy Policy forms part of our approach to providing that information, and in some cases, we may provide additional or more specific collection notices.

4. Why we collect, hold, use and disclose personal information

We collect, hold, use and disclose personal information for the primary purposes of providing education, care and related services, and for other purposes connected with the School's functions and activities.

We may also use and disclose personal information for secondary purposes where those purposes are related to the primary purpose and would be reasonably expected by the individual, or where otherwise permitted or required by law.

These include:

Students and parents

- providing Montessori education and related services
- meeting the needs of parents, students and the School throughout the whole period a student is enrolled at the School
- day-to-day administration of the school
- administering enrolment, attendance, learning support and wellbeing
- communicating with students and families
- complying with legal obligations, responding to lawful requests (e.g., child safety / mandatory reporting), and making required reports to government authorities
- maintaining student and workplace safety and fulfilling our duty of care
- managing staff, contractors and volunteers
- maintaining ICT systems, cybersecurity and records management
- managing student health, wellbeing, and safety, including responding to medical needs and fulfilling our duty of care obligations.

Volunteers

- to contact you about, and administer, the volunteer position
- for insurance purposes
- satisfying the School's legal obligations, for example, in relation to child protection legislation.

Job applicants and contractors

- assessing and (if successful) engaging the applicant or contractor
- administering the individual's employment or contract
- for insurance purposes
- satisfying the School's legal obligations, for example, in relation to child protection legislation

If we do not receive certain information, we may be unable to properly provide education services, meet duty of care obligations, or comply with legal requirements.

5. Who we disclose personal information to

The School may disclose personal information, including sensitive information such as health information, for purposes related to education, care, safety, and administration, and to seek support and professional advice where appropriate. This may include to:

- other schools and teachers at those schools, including a new school to which a student transfers to facilitate the transfer of the student;
- government departments (including for policy and funding purposes);
- medical practitioners;
- people providing educational, support and health services to the School, including specialist visiting teachers, sports coaches, volunteers, and counsellors;
- providers of specialist advisory services and assistance to the School, including in the area of Human Resources, child protection, students with additional needs and for the purpose of administering Microsoft365 products and ensuring their proper use (see further the section below 'Overseas Disclosure of Personal Information');
- providers of learning and assessment tools;

- assessment and educational authorities, including the Australian Curriculum, Assessment and Reporting Authority (ACARA) and NAPLAN Test Administration Authorities (who will disclose it to the entity that manages the online platform for NAPLAN);
- agencies and organisations to whom we are required to disclose personal information for education, funding and research purposes;
- people providing administrative and financial services to the School;
- the provider of our information management and storage system and other information technology services;
- recipients of School publications, such as newsletters and magazines;
- students' parents or guardians;
- anyone you authorise the School to disclose information to;
- anyone to whom we are required or authorised to disclose the information to by law, including child protection laws.

6. Key systems and platforms we use

We store your personal information in hard copy and electronically. To operate effectively, we use a small number of core platforms:

(a) Sentral – Student Information Management System (SIMS)

We use Sentral to manage student administration and records.

(b) Microsoft 365 (M365) – student and staff accounts

We use Microsoft 365 for school email accounts and productivity tools such as OneDrive. Student email addresses are configured to not use full names and are designed primarily for logging into school devices and saving work. (Even where identifiers are reduced, this may still be personal information if a student is reasonably identifiable.)

(c) Transparent Classroom – Montessori learning, assessment and reporting platform

We use Transparent Classroom with a minimal identification approach, generally recording students as first name + surname initial only and not entering additional identifiers (e.g., full date of birth).

Transparent Classroom states in its published privacy policy that it stores personal information on servers located in the United States.

(d) Facebook and Instagram – social media platforms

We use Facebook and Instagram to communicate with families, share updates, and promote the School.

We limit the personal information shared on these platforms and follow internal guidelines regarding images and identifying information. However, content published on social media may be accessed by a broad audience and may be stored or processed outside Australia.

Meta (the company that operates Facebook and Instagram) processes data across its global infrastructure, including in the United States and other countries.

(e) eNudge – email communications platform

We use eNudge to send newsletters and updates to families and community members.

Mailing lists typically include names and email addresses provided voluntarily by parents, guardians, or interested parties.

eNudge is an Australian-owned and Australian-hosted email communications platform. eNudge states that contact information is stored securely on Australian servers and kept within Australia, in accordance with its privacy policy.

(f) MYOB – accounting, payroll and finance system

We use MYOB to manage the School's accounting, payroll, and financial administration.

This system contains personal information relating to employees, and limited financial information relating to families (such as billing records where relevant).

MYOB services for Australian customers are primarily hosted in Australia. However, some supporting services and technical processing may occur outside Australia as part of system operation and support.

(g) Calendly – booking and scheduling tool

We use Calendly to allow parents and prospective families to book tours, meetings, or appointments with the School.

Calendly may collect personal information such as name, email address, and booking details when appointments are made.

Calendly is a United States-based service and stores information on servers located in the United States, with some processing potentially occurring in other regions.

(h) WordPress – website platform

The School uses WordPress to host and manage its public website.

Depending on the specific configuration (including hosting provider and plugins), WordPress sites may collect personal information such as names, email addresses, and enquiry form submissions.

Data storage and processing for WordPress websites depend on the chosen hosting provider and any integrated services, and may occur in Australia or overseas (including the United States or other regions).

7. Overseas disclosure of personal information

We use a range of trusted third-party platforms to operate the School, and while most core systems store data in Australia, some services may involve storing or processing personal information overseas as part of their normal operations.

For example:

- Transparent Classroom indicates that personal information is stored on servers located in the United States.
- Other platforms we use (such as social media, booking tools, and communication services) may also involve overseas data processing and/or storage depending on how those services operate.
- Microsoft 365 data used by the School is stored at rest primarily in Australia, with some collaboration services (such as Microsoft Teams) operating within the Asia-Pacific region. School personnel and its service providers may have the ability to access, monitor, use or disclose emails, communications (e.g., instant messaging), documents and associated administrative data for the purposes of administering Microsoft 365 products and ensuring their proper use.

Where the School discloses personal information to an overseas recipient, we take reasonable steps to ensure that the recipient handles the information in a manner consistent with the Australian Privacy

Principles. This may include due diligence of service providers and reliance on contractual, technical, and organisational safeguards.

In some circumstances, we may seek consent to disclose personal information to overseas recipients. By providing personal information to the School, you acknowledge that your information may be disclosed to overseas service providers as described in this policy.

Overseas recipients may not be subject to privacy laws that are equivalent to those in Australia. However, we take reasonable steps to ensure appropriate safeguards are in place to protect personal information.

8. Images, photographs and videos

Photographs and videos can be personal information. We handle images carefully and seek consent where appropriate—particularly for any public-facing use (e.g., website, public social media) where a student is identifiable.

Where photos/videos are shared only within the school community (e.g., via school platforms restricted to families/staff), this is generally done consistent with our collection notices and community expectations; for broader publication we will generally seek express permission.

9. Generative AI and personal information

Students do not access generative AI tools as part of their education at the School.

The School permits administrative use of Microsoft Copilot (within our Microsoft 365 environment) subject to strict rules, including:

- not entering any personal, sensitive, or confidential information about students, staff, or families into public generative AI tools
- using approved tools only (Microsoft Copilot is the approved tool)
- AI tools not making decisions about students; staff remain responsible for all decisions
- the School informing users about data collection and seeking consent where needed.

We do not use AI for automated decision-making that significantly affects students' rights or interests. If this changes, we will update this policy accordingly (noting additional transparency requirements apply from 10 December 2026 for certain automated decision-making).

For further information, see the School's Generative AI Usage Policy.

10. Keeping information accurate and up to date

Under the Commonwealth Privacy Act and the NSW Health Records Act, an individual has the right to seek access to, and/or correction of, any personal information which the School holds about them. Students will generally be able to access and update their personal information through their Parents.

There are some exceptions to these rights set out in the applicable legislation.

To make a request to access, update or correct any personal information the School holds about you or your child, please contact the School Principal by email, post or telephone as listed under section 13 of this policy. The School may require you to verify your identity and specify what information you require.

We will respond to requests for access or correction within a reasonable period, and will take reasonable steps to provide access in the manner requested where practicable.

The School may charge a reasonable fee for giving access to your personal information (but will not charge for the making of the request or to correct your personal information). If the information sought is extensive, the School will advise the likely cost in advance.

If we decide to refuse your request, we will provide you with written notice explaining the reasons for refusal (unless, in light of the grounds for refusing, it would be unreasonable to provide reasons) and how to complain.

11. Consent and rights of access to the personal information of students

The School respects every Parent's right to make decisions concerning their child's education.

Generally, the School will refer any requests for consent and notices in relation to the personal information of a student to the student's Parents. Generally, the School will treat consent given by Parents as consent given on behalf of the student and notice to Parents will act as notice given to the student. Parents may seek access to personal information held by the School about them or their child by contacting the School Principal by telephone or in writing. However, there may be occasions when access is denied. Such occasions may include (but are not limited to) where the School believes the student has capacity to consent and the School is not permitted to disclose the information to the Parent without the student's consent, where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of the School's duty of care to the student.

The School will generally deal with parents or guardians in relation to a student's personal information, particularly given the primary school context and the age of students.

However, as students develop and where appropriate in the circumstances, the School may involve students in decisions relating to their personal information, taking into account their age, maturity and understanding.

In limited circumstances, the School may be required to consider a student's capacity to make decisions about their personal information, in accordance with applicable laws.

12. Data security, retention and disposal

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification and disclosure. This includes:

- access controls and least-privilege access
- secure systems and device management practices
- staff training and confidentiality expectations
- due diligence and contracts with service providers.

We also take reasonable steps to destroy or de-identify personal information when it is no longer needed for any lawful purpose.

In determining how long to retain personal information, we consider our legal obligations, including education, child protection, employment, and health record requirements, as well as operational needs such as maintaining student records and responding to enquiries.

In some cases, we may be required to retain personal information for extended periods. Where information is no longer required, we securely destroy or de-identify it.

13. Data breaches

If a data breach occurs, we follow a documented response process to:

- contain the breach
- assess whether it is likely to result in serious harm
- notify affected individuals and the Office of the Australian Information Commissioner (OAIC) where required under the Notifiable Data Breaches scheme.

We maintain internal procedures to identify, assess and respond to suspected data breaches.

14. Related documents

- Child Protection Policy & Procedures
- Enrolment and Orientation Policy
- Generative AI Usage Policy
- Medical Conditions Policy
- Risk Management Policy
- Social Networking Policy
- Student and Volunteer Policy
- Use of Information Technology, Computer, Telephone and Equipment Code of Use

15. Making a privacy complaint

If you believe the School has mishandled personal information or breached its privacy obligations, you can lodge a complaint by contacting the Principal. Please include as much detail as possible.

We will:

- acknowledge receipt of your complaint
- investigate and respond within a reasonable timeframe
- take steps to remedy any issues identified.

Privacy contact: Principal
Email: principal@southsidemontessori.edu.au
Phone: (02) 9533 1229

If you have any concerns or questions about privacy, please contact the Principal using the details above.

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC): https://www.oaic.gov.au/

15. Updates to this policy

This Privacy Policy will be reviewed at least annually and may be updated from time to time, including when we introduce new systems or significantly change how we handle information. The current version will be available on our website, is easily accessible and free of charge

16. Version Control

Version	Approved Date	Details	Approved By

1.0	22 May 2026	Initial version of Privacy Policy	Board