



The Montessori School Kingsley Inc.

INFORMATION SECURITY POLICY



1. VERSION MANAGEMENT

Version	Date Published/Reviewed	Changes	Author	Date Ratified by School Board
1	01/01/2004			
2	23/3/2018	Update Policy as per changes to Privacy Act	Principal	April 2018
3	2026	Name Change from Privacy and Media Policy to Information Security Policy, Updating and Benchmarking + Created new procedures: Privacy Management Procedures, Records Management Procedures, and Incident and Breach Management Procedures.	Principal	23 February 2026

2. INTENT

The School is committed to protecting the privacy of individuals in our community, managing personal information with care and transparency, and maintaining accurate and secure records.

This Information Security Policy outlines how the School:

- Collects, uses, stores, and discloses personal information in line with the Australian Privacy Principles under the Privacy Act 1988 (Cth).
 - Identifies, manages, and reports privacy and data breaches in accordance with legal and regulatory requirements.
 - Identifies, manages, and documents operational incidents, including loss of utilities and failures of critical systems.
 - Creates, maintains, and securely disposes of records to meet legal, regulatory, and operational requirements.

This Policy ensures:

- Information is handled lawfully, confidentially, and with respect.
- Records support accountability, compliance, and effective decision-making.
- Data Breaches, including information security and cyber events are responded to promptly to minimise harm and meet statutory reporting obligations.
- Operational incidents are managed swiftly to maintain safety, communication, and continuity of School operations.
- The School meets all relevant reporting obligations.

It also promotes a culture of:

- Accountability – Staff understand their responsibilities in managing data and records.
- Improvement – Incidents are reviewed to strengthen practices.
- Urgency – Timely action ensures risks are minimised and obligations are met.

3. ORGANISATIONAL SCOPE

This Policy applies to all students, parents, employees, volunteers, contractors, and third-party service providers associated with the School. It covers all personal information collected, held, used or disclosed by the School.

Where the School engages third-party service providers to collect, store or process personal information on its behalf, this Policy continues to apply. The School remains responsible for ensuring appropriate privacy and information security controls are implemented and maintained.

By engaging with the School or providing personal information, individuals acknowledge and consent to the collection, use, and disclosure of their personal information in accordance with this Policy.

3.1 Policy Exemptions

Certain disclosures are handled under specific legislation or policies and are exempt from this Policy, including:

- Public Interest Disclosures under the Public Interest Disclosures Act 2003;
- Staff or student complaints;
- Reportable Allegations under the Critical Incident Management Policy;
- Incidents and hazards under the Health and Safety Policy.
- Employee records related to current or former employment relationships, which are exempt from the Australian Privacy Principles under the Privacy Act 1988 (Cth).
 - This exemption exists because employment relationships are governed by separate legislation and frameworks, such as:
 - Fair Work Act 2009
 - Workplace relations law
 - Enterprise agreements and awards

4. DEFINITIONS

TERM	DEFINITION
Australian Privacy Principles	The Australian Privacy Principles (or APPs) are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers.
Board	The governing board of The Montessori School Kingsley, comprises its Chairperson, the Principal, Directors, and Heritage Directors.
Breach	A serious failure to meet a legal, regulatory, or contractual responsibility. Significant or material breaches are generally reportable to the regulator(s).
Consent	The voluntary and informed agreement given by an individual regarding the collection, use, and disclosure of their personal information by the School. Consent should be provided freely, specific to the intended purposes, and can be withdrawn at any time.
Employee Records	Records directly related to a current or former employment relationship are excluded from the Australian Privacy Principles.
Incident (for this Policy, we are referring to operational incidents)	An unplanned disruption to School operations, such as loss of utilities or failure of critical systems, that does not involve unauthorised access to personal information.
Incident Register	A centralised repository or database used to record and track details of incidents, including their nature, severity, date and time of occurrence, stakeholders involved, actions taken, and resolution status.
Incident Response Plan	A structured framework or set of procedures outlining the steps to be taken in response to different types of incidents, including roles and responsibilities, communication protocols, escalation procedures, and recovery strategies.
Loss	Accidental or inadvertent loss of personal information held by the School, in circumstances where it is likely to result in unauthorised access or disclosure.

Notifiable Data Breaches (NDB) Scheme	The Notifiable Data Breaches (NDB) Scheme is part of the Privacy Act 1988 (Cth) and requires organisations covered by the Act to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm. The notification must include recommendations on steps individuals should take in response to the breach.
Office of the Australian Information Commissioner (OAIC)	An independent Australian Government agency, acting as the national data protection authority for Australia, established under the Australian Information Commissioner Act 2010,[3] headed by the Australian Information Commissioner.
Parents/Guardians	Individuals who have legal responsibility for a student at the School. This includes biological parents, adoptive parents, legal guardians, or individuals with parental responsibility as recognised by relevant laws and regulations.
Personal Information	Any information that identifies or can reasonably identify an individual. It includes, but is not limited to, names, addresses, phone numbers, email addresses, photographs, social security numbers, student identification numbers, or any other information that can be linked to a specific person.
Privacy Act	The Privacy Act (1988) includes the Privacy Amendment (Private Sector) Act 2000 and Privacy Amendment (Notifiable Data Breaches) Act 2017.
Record	‘Document’ or an ‘electronic or other device’. A ‘document’ includes anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.
School	The Montessori School Kingsley
Sensitive Information	A subset of personal information, including racial or ethnic origin, political opinions, religious beliefs, health information, and criminal records.
Students	Individuals who are enrolled or registered at the School. This term covers both current and former students.
Third Parties	Individuals, organisations, or entities that are not directly affiliated with the School. They can include external service providers, vendors, contractors, educational partners, or any other parties with whom the school may interact or share personal information.
Workers	The person who carries out work in any capacity for the School, including work as: a. an employee; or b. a contractor or subcontractor; or c. an employee of a contractor or subcontractor; or d. an employee of a labour hire company who has been assigned to work in the person’s business or undertaking; or e. an apprentice or trainee; or f. a student gaining work experience; or g. a volunteer.

5. POLICY CONTENT

5.1 Privacy Management

The School is committed to protecting the personal information of everyone in our community. We handle all personal data in accordance with relevant privacy laws and principles, and we make every effort to ensure that your information is collected, used, and stored responsibly.

5.1.1 Privacy Principles

- The School is committed to collecting and handling personal information responsibly, in line with privacy laws, to protect individuals' privacy.
- Personal information is collected for educational and administrative purposes and is safeguarded with great care.
- Information is collected in a clear, lawful, and responsible manner, ensuring compliance with privacy laws.
- Personal information is used only for the purpose it was collected and related purposes reasonably expected or consented to.
- The School does not use Government identifiers as personal identifiers, and any use or disclosure complies with the Privacy Act.
- Personal and sensitive information is disclosed only for the purposes it was collected, as required by law, or with consent.
- The School ensures secure management of personal information, maintaining confidentiality and implementing processes for access or updates.
- Parents and students have the right to consent to and access their personal information in accordance with privacy laws.
- Individuals have the right to access, correct, or request the deletion of their personal information held by the School, subject to applicable legal exceptions.
- Third-party providers with access to personal information must agree to comply with this Policy and relevant privacy laws through formal agreements or contracts.
- Individuals can raise privacy concerns by contacting the Principal or lodging a formal complaint via the School's Complaints Management Policy and Procedures.

5.2 Records Management

The School recognises the importance of effective and secure records management to support its operations, ensure regulatory compliance, and safeguard the privacy of individuals. This section outlines how the School manages records related to employment, students, and other operational matters throughout their lifecycle—from creation and use to retention and disposal.

5.2.1 Records Management Principles

The School follows the below key principles in managing physical and digital records:

- Records are created and maintained in an accurate, consistent, and timely manner to reflect the School's operations and meet legal requirements.
- Records are retained for the required periods, in accordance with legislative, regulatory, and contractual obligations.
- Records are securely stored to protect against unauthorised access, alteration, loss, or damage. Only authorised individuals may access records.
- Staff can access and update records where appropriate, following relevant privacy legislation and School policies.
- When no longer required, records are securely destroyed or de-identified in accordance with legal and internal requirements.
- The School regularly audits its records management practices to ensure adherence to these principles and policies.

5.3 Incident Management

The School recognises that operational incidents, such as loss of utilities or failure of critical systems, can significantly affect safety, communication, and core school functions. The School manages incidents through timely identification, escalation, response, and documentation.

5.3.1 Incident Types Covered

This section applies to incidents that disrupt normal operations, including but not limited to:

A. Loss of Utilities

- Water supply failure
- Sewerage system failure
- Power outage
- Internet or network outage

B. Failure or Outage of Critical Systems

- Microsoft 365 (email, document storage, authentication)
- SchoolStream (communication app)
- Civica (student management system)
- Any other essential digital platform required for operations, learning, communication, or compliance

5.3.2 Incident Management Principles

- Incidents are identified and reported as quickly as possible to minimise disruption.
- The School follows a structured response process to ensure safety, continuity of operations, and timely communication.
- Relevant staff (e.g., ICT support, leadership, administration) are notified depending on the nature and severity of the incident.
- Where an incident presents a risk to safety (e.g., sewerage issues, water shortages), appropriate emergency procedures are activated.
- The School communicates with staff, parents, and students as needed, using alternative channels if usual systems are unavailable.
- All incidents are recorded in the Incident Register and reviewed for continuous improvement and risk mitigation.

5.4 Breaches Management

The School takes a proactive and transparent approach to managing breaches, recognising their potential impact on individuals and the broader school community. This Policy supports compliance with legal obligations and continuous improvement through prevention, timely response, and effective communication.

5.4.1 Breach Management Principles

- The School takes immediate and appropriate action in the event of a suspected breach to assess and address the impact on individuals and the School.
- All breaches are identified, reported, and investigated in line with legal and regulatory requirements.
- Where necessary, breaches are reported to relevant authorities in accordance with the Notifiable Data Breaches Scheme.
- The School works to prevent future breaches by reviewing and improving security measures and processes.
- Staff and community members are trained to recognise potential breaches and to escalate issues promptly.
- The School maintains a Breach Response Plan outlining detailed steps for managing privacy and data breaches.
- Records of all breaches and breach investigations are maintained securely in the Incident Register for auditing, analysis, and continuous improvement.
 - The Incident Register is maintained by the Principal or delegate and is reviewed regularly to identify patterns and ensure accountability.

5.4.2 Reporting Obligations

Where a privacy breach is assessed as likely to result in serious harm, the School will notify affected individuals and the Office of the Australian Information Commissioner (OAIC) in accordance with the requirements of the Privacy Act 1988 (Cth) and the Notifiable Data Breaches Scheme.

6. ACCOUNTABILITIES AND RESPONSIBILITIES

In relation to this Policy, the following positions are responsible for:

ROLE	RESPONSIBILITY
Policy Owner	The Policy Owner, the School Board, is responsible for the cyclical review and approval of this Policy.
School Board	The Board provides oversight of information privacy and breach management practices and ensures the School's legal obligations are met.
Principal	The Principal is responsible for ensuring that the requirements of this Policy are implemented, monitored, and reviewed.
Workers	Ensuring they understand the information presented in this Policy.

7. RELATED DOCUMENTS

7.1 Policies that are relevant to the operation of this Policy are as follows:

- Enrolment Policy
- Complaints Management Policy
- Critical Incident Management Policy

7.2 Procedures that are relevant to the operation of this Policy are as follows:

- Enrolment and Resignation Procedures
- Complaints Management Procedures
- Critical Incident Management Procedures
- Privacy Management Procedures
- Records Management Procedures
- Incident and Breach Procedures

7.3 Internal documents that are relevant to the operation of this Policy are as follows:

- Staff Code of Conduct
- Student Code of Conduct
- Community Code of Conduct
- Notifiable Data Breach Register
- Photograph Permission Form

7.4 External documents that are relevant to the operation of this Policy are as follows:

- Australian Privacy Principles
- Privacy Act 1988 (Cth)
- School Education Act 1999
- State Records Act 2000 (WA)