

Privacy and Confidentiality policy

PURPOSE

This policy provides clear guidelines for:

- The collection, storage, use, disclosure, and disposal of personal, sensitive, and health information, including photographs and videos
- Compliance with privacy legislation and sector regulations
- Responding to requests for information to promote child wellbeing or safety and/or manage family violence risk
- Sharing and requesting information under the Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS)

POLICY STATEMENT

MEYM is committed to:

- Responsible and secure handling of personal and health information
- Protecting the privacy of all individuals, including children, families, staff, and visitors
- Ensuring transparency and informed consent in all data practices
- Proactively sharing information to promote child wellbeing and safety, consistent with best interests
- Complying with all relevant legislation, including the National Model Code for image use

BACKGROUND AND LEGISLATION

Children have the right to feel safe, respected, and protected in all aspects of their early learning environment—including how their personal information is collected, stored, and shared. In early childhood settings, privacy is not just a legal obligation—it's a foundational element of child safety, dignity, and trust.

Personal, sensitive, and health information—including photographs and videos—is increasingly stored and shared through digital platforms. Without clear safeguards, this information can be misused, misunderstood, or accessed inappropriately. Children are particularly vulnerable to breaches of privacy, as they rely on adults to protect their identity, wellbeing, and personal boundaries.

Privacy breaches can have serious consequences. They may expose children and families to reputational harm, emotional distress, or even physical risk. Inappropriate sharing of information—whether intentional or accidental—can undermine relationships between educators and families, compromise child safety, and breach legal obligations.

The key to privacy in the early years is prevention. The most effective protection comes from creating a service culture that is transparent, respectful, and proactive. This includes:

- Teaching children what personal information is and why it matters
- Ensuring staff understand their legal and ethical responsibilities
- Building systems that safeguard data and limit access
- Responding swiftly and respectfully to any concerns or breaches

MEYM's Privacy and Confidentiality Policy is grounded in Victorian and Commonwealth legislation, including:

- Privacy Act 1988 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Education and Care Services National Law and Regulations

- Child Information Sharing Scheme (CISS)
- Family Violence Information Sharing Scheme (FVISS)
- National Model Code for image and video use

These laws and frameworks work together to ensure that children's personal information is protected, shared only when necessary, and handled with care. MEYM is committed to upholding these standards and fostering a privacy-conscious culture that supports every child's right to safety and respect.

SCOPE

This policy applies to:

- Approved Provider, Nominated Supervisor, Persons in Day-to-Day Charge
- Early childhood teachers, educators, staff, students, volunteers
- Parents/guardians, children, contractors, and visitors
- All programs and activities, including offsite excursions

COLLECTION, USE AND DISCLOSURE OF INFORMATION

MEYM collects personal, sensitive, and health information for:

- Providing education and care
- Managing service operations
- Employment and volunteer engagement
- Legal and funding obligations

Disclosure may occur to:

- Government departments, local authorities, law enforcement
- Health organisations in emergencies
- Information Sharing Entities under CISS/FVISS
- Individuals authorised by the data subject

Details are outlined in Attachment 4: Privacy Statement.

IMAGE AND MEDIA USE

Photographs and videos are treated as personal information. MEYM:

- Uses only service-issued devices for image capture
- Stores media securely and deletes when no longer required
- Seeks written consent for all external publication use
- Respects cultural sensitivities and child/family preferences
- Follows the National Model Code and MEYM's Safe Use of Digital Technologies Policy

RECORD KEEPING AND RETENTION

MEYM maintains secure physical and digital storage systems. Records are retained per regulatory requirements, as detailed in Attachment 1, including:

- Enrolment, attendance, incident, and medication records
- Staff and volunteer documentation
- Records relevant to child safety and wellbeing (retained for 45 years)
- Secure disposal protocols for hardcopy and digital data

ACCESS AND COMPLAINTS

Individuals may access or correct their personal information in accordance with legislation. Complaints are managed under MEYM's Dealing with Complaints Policy and may be escalated to the Office of the Australian Information Commissioner (OAIC) if unresolved.

INFORMATION SHARING UNDER CISS AND FVISS

MEYM shares information to promote child wellbeing and safety or manage family violence risk. Key principles:

- Apply the threshold test before sharing
- Use professional judgment and respect cultural identity
- Consent is not required for sharing about children or perpetrators
- Maintain accurate records of all requests and disclosures

Follow procedures outlined in Attachment 7

ROLES AND RESPONSIBILITIES

Approved Provider and Persons with Management or Control are responsible for governance, oversight, and strategic leadership of privacy compliance.

They must:

- Ensure MEYM complies with all relevant privacy legislation and information sharing schemes
- Oversee secure systems for data collection, storage, access, and disposal
- Authorise access to personal and sensitive information and approve exemptions where appropriate
- Ensure staff only use service-issued devices for capturing and storing images or videos
- Investigate and respond to privacy breaches, including escalation to the OAIC or Regulatory Authority
- Ensure staff complete annual privacy training and sign confidentiality declarations
- Monitor compliance with the National Model Code and MEYM's Privacy and Confidentiality Policy
- Embed a culture of transparency, respect, and lawful information handling across the organisation

Nominated Supervisors and Persons in Day-to-Day Charge are responsible for operational implementation of privacy practices and supervision of staff.

They must:

- Implement privacy procedures in daily practice, including secure handling of enrolment and health records
- Monitor staff use of service-issued devices and ensure appropriate access controls
- Support staff to comply with image use protocols and obtain parental consent

- Respond promptly to privacy concerns, breaches, or complaints
- Ensure families are informed about their rights to access and correct personal information
- Facilitate staff access to secure cloud platforms for storing service-related files
- Maintain accurate records of disclosures made under CISS and FVISS
- Ensure monitoring systems (e.g. file audits, password logs) are in place and reviewed regularly

Early Childhood Teachers, Educators and all other staff are responsible for safe, ethical, and lawful handling of personal and sensitive information.

They must:

- Treat all personal information with professionalism and confidentiality
- Use only service-issued devices for capturing images or videos of children
- Ask children for permission before taking photos or videos and explain their use
- Store all documentation securely and never transfer service-related files to personal devices
- Report suspected breaches or inappropriate sharing of information immediately
- Maintain security of passwords, files, and devices
- Ensure families only access records relating to their own child
- Comply with MEYM's Privacy and Confidentiality Policy and all related procedures

Families play a vital role in supporting the MEYM's privacy and confidentiality standards.

They must:

- Provide accurate and up-to-date personal information during enrolment
- Provide written consent for image and video use where required
- Respect service policies by not taking photos or videos of other children or staff
- Avoid sharing service-captured images on personal social media platforms
- Communicate openly with staff about privacy concerns or changes to custody arrangements
- Support children's understanding of privacy and responsible information sharing

Contractors, volunteers, visitors and students are required to comply with all aspects of MEYM's policies.

DEFINITIONS

A glossary of definitions can be found on our website.

POLICY REVIEW

To ensure the values and objectives of this policy are effectively met, the Approved Provider will implement a continuous evaluation process. This includes regularly seeking feedback from all stakeholders impacted by the policy, monitoring its implementation, compliance, and any related complaints or incidents. The policy will be kept current with relevant legislation, research, and best practice, and revised as part of the service's scheduled review cycle or when necessary. In accordance with Regulation 172(2), all affected stakeholders will be notified at least 14 days prior to any significant changes to the policy or its procedures, unless a shorter timeframe is required due to potential risk.

Approving Authority	General Manager
Date Approved	September 15 th 2025
Date Effective	September 22 nd 2025
Policy Owner	MEYM
Policy Category	Mandatory Policy
Edition	V1
Review Date	September 2026

Attachment 1: Record Keeping and Privacy Laws

OVERVIEW

Early childhood services must ensure that all processes for collecting, storing, using, disclosing, and disposing of personal, sensitive, and health information comply with:

- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)
- Privacy Act 1988 (Cth)
- Education and Care Services National Law and Regulations

This includes enrolment forms, attendance records, medication and incident reports, images and videos, and electronic or hardcopy documentation.

EXAMPLES OF RECORDS IMPACTED BY PRIVACY LEGISLATION

- **Enrolment Records** Must include personal details, parenting orders, and medical conditions (Regulations 160–162). These are classified as personal, sensitive, and health information and must be stored securely.
- **Attendance Records** Must include child's full name, arrival/departure times, and signatures (Regulation 158). Emergency contact details may be stored separately in a sealed envelope or folder.
- **Medication and Incident Records** Must include health-related information and be retained securely (Regulations 87 and 92).
- **Images and Videos** Classified as personal information. Must be stored securely, geotagging disabled, and disposed of appropriately when no longer required.
- **Electronic Records** Must be stored in password-protected folders or platforms. Access must be restricted to authorised personnel. Passwords must be securely recorded and stored.
- **Off-Site Documentation** Confidential information taken off-site (e.g. for excursions) must be transported and stored securely.
- **Forms** All forms collecting personal, sensitive, or health information must include MEYM's Privacy Statement (see Attachment 4).
- **Data Minimisation** MEYM will only collect information that is necessary and has a specific, immediate purpose. Information with no current use will not be collected.

RECORD RETENTION TIMEFRAMES

The following records must be kept securely and be readily accessible to authorised officers. Retention periods are based on regulatory requirements and child safety obligations.

Type of Record	Responsibility	Retention Period
Insurance policies (if not government-provided)	Approved Provider	Ongoing
Quality Improvement Plan	Approved Provider	Ongoing, revised annually
Child assessments/evaluations	Approved Provider	3 years after last attendance

Type of Record	Responsibility	Retention Period
Incident/injury/trauma/illness records	Approved Provider	Until child is 25 years old
Records relevant to child safety/wellbeing (e.g. abuse disclosures)	Approved Provider	At least 45 years
Medication records	Approved Provider	3 years after last attendance
Attendance records	Approved Provider	3 years after last attendance
Enrolment records	Approved Provider	3 years after last attendance
Death of a child	Approved Provider	7 years after death
Compliance history	Approved Provider	3 years after service operation ends
Transportation records (centre-based services)	Approved Provider / Nominated Supervisor	3 years after last attendance
Staff records	Approved Provider	3 years after employment ends
Replacement educator records	Approved Provider	3 years after employment ends
Replacement ECT/suitably qualified person	Approved Provider	3 years after employment ends
Access to ECT/suitably qualified person	Approved Provider	3 years after employment ends
Educators working directly with children	Approved Provider	3 years after employment ends
Volunteers/students (including WWCC details)	Approved Provider	3 years after attendance ends
Responsible person in day-to-day charge	Approved Provider	3 years after employment ends

Attachment 2: Privacy Principals in Action

OVERVIEW

MEYM complies with multiple privacy frameworks depending on the nature of its operations and contractual obligations. These include:

- Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth)
- Information Privacy Principles (IPPs) under the Privacy and Data Protection Act 2014 (Vic)
- Health Privacy Principles (HPPs) under the Health Records Act 2001 (Vic)

As MEYM operates under a Victorian government contract and collects health information, more than one framework may apply simultaneously. The Child Information Sharing Scheme (CISS) and Family Violence Information Sharing Scheme (FVISS) modify certain privacy obligations to enable safe, lawful information sharing.

PRINCIPLES IN PRACTICE

Australian Privacy Principles (APPs)	Information Privacy Principles (IPPs)	Health Privacy Principles (HPPs)	MEYM Practice
APP 1 – Open and transparent management of personal information	IPP 5 – Openness	HPP 5 – Openness	MEYM maintains an up-to-date Privacy and Confidentiality Policy, available to all stakeholders upon request.
APP 2 – Anonymity and pseudonymity	IPP 8 – Anonymity	HPP 8 – Anonymity	Where lawful and practicable, individuals may remain anonymous (e.g. surveys, feedback forms).
APP 3 & 4 – Collection of solicited and unsolicited personal information	IPP 1 & 10 – Collection and Sensitive Information	HPP 1 – Collection	MEYM collects only the personal, sensitive, and health information necessary for service delivery. Information is collected via enrolment forms, medical plans, attendance records, and staff documentation.
APP 5 & 6 – Notification and use/disclosure of personal information	IPP 2 – Use and Disclosure	HPP 2 – Use and Disclosure	MEYM informs individuals why information is collected, how it will be used, and who it may be disclosed to. Consent is obtained where required.

MODIFICATIONS UNDER CISS AND FVISS

MEYM acknowledges that under CISS and FVISS:

- Information may be collected from other Information Sharing Entities (ISEs) without notifying the individual, if notification would compromise child safety or wellbeing
- Consent is not required to share personal or sensitive information under the scheme when promoting child wellbeing or managing family violence risk
- Information sharing must be respectful of cultural identity, vulnerability, and the child's best interests
- MEYM maintains accurate records of all information shared under the scheme

