PRIVACY AND CONFIDENTIALITY

QUALITY AREA 7 | ELAA VERSION 1.7

PURPOSE

This policy provides a clear set of guidelines:

- for the collection, storage, use, disclosure, and disposal of personal information, including photos, videos, and health information at Somerville Kindergarten
- to ensure compliance with privacy legislation
- on responding to requests for information to promote child wellbeing or safety and/or assess and manage risk of family violence (mandatory)
- on sharing and requesting information to promote child wellbeing or safety and/or manage risk of family violence.

POLICY STATEMENT

VALUES

Somerville Kindergarten is committed to:

- responsible and secure collection and handling of personal (including photos and videos), and health information
- protecting the privacy of each individual's personal information (including photos and videos),
- ensuring individuals are fully informed regarding the collection, storage, use, disclosure, and disposal of their personal (including photos and videos), and health information, and their access to that information
- proactively sharing information to promote the wellbeing and/or safety of a child or a group of children, consistent with their best interests

SCOPE

This policy applies to the approved provider, persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, parents/guardians, children, and others attending the programs and activities of Somerville Kindergarten, including during offsite excursions and activities.

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
R indicates legislation requirement, and should not be deleted					
1. Ensuring all records and documents (including images and videos) are maintained and stored in accordance with *Regulations 177, 181 and 183* of the *Education*	R	√	√		√

and Care Services National Regulations 2011 and *National Law 175*					
2. Ensuring the service complies with the requirements of the *Health Privacy Principles* as outlined in the *Health Records Act 2001*, the *Information Privacy Principles* as outlined in the *Privacy and Data Protection Act 2014 (Vic)* and, where applicable, the *Australia Privacy Principles* as outlined in the *Privacy Act 1988 (Cth)* and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)*, by taking proactive steps to establish and maintain internal practices, procedures, and systems that ensure compliance with privacy legalisations including: • identifying the kind of personal, sensitive, and health information that will be collected from an individual or a family • communicating the reason why personal, sensitive, and health information is being collected, and how it will be stored, used, and disclosed, and managed and are provided with the service's privacy statement *(refer to Attachment 4)* and all relevant forms • communicating how an individual or family can access and/or update their personal, sensitive, and health information at any time, to make corrections or update information *(refer to Attachment 4)* • how children's personal information (including photos and images) is being shared online or through apps • communicating how an individual or family can complain about any breaches of the privacy legislation, and how the service will deal with these complaints	R	√			
3. Ensuring a copy of this policy, including the Privacy Statement, is provided to all stakeholders, is prominently displayed at the service and/or electronically accessible, is up to date and available on request	R	√			
4. Reading and acknowledging they have read the *Privacy and Confidentiality Policy,* including the Privacy Statement *(refer to Attachments 3 & 4 as applicable)*	R	√	√	√	√
5. Maintaining the management of privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification	R	√	√		
6. Protecting personal information from misuse, interference, loss and unauthorised access, modification or disclosure, as well as unauthorised access, modification or disclosure.	R	√	√		
7. Identifying and responding to privacy breaches, handling access and correction requests, and receiving and responding to complaints and inquiries	R	√			
8. Providing regular staff training and information on how the privacy legislation applies to them and the service	R	√			
9. Ensuring appropriate supervision of staff who regularly handle personal, sensitive, and health information	R	√			

10. Ensuring that personal, sensitive, and health information is only collected by lawful and fair means, and is accurate and complete	R	√	√		
11. Teaching children what personal information is and why they should be very careful about sharing this information online	R	√	√	√	√
12. Ensuring parents/guardians know why personal, sensitive and health information is being collected and how it will be used, disclosed and managed and are provided with the service's Privacy Statement *(refer to Attachment 4)* and all relevant forms	R	√	√		
13. Ensuring that an individual or family can have access to their personal, sensitive and health information at any time, to make corrections or update information *(refer to Attachment 4)*	R	√	√	√	√
14. Providing adequate and appropriate secure storage for personal (including photos and videos), sensitive, and health information collected by the service, including electronic storage *(refer to Attachment 2)*	R	√			
15. Ensuring that records and documents are kept in accordance with *Regulation 183*	R	√	√		
16. Taking reasonable steps to securely destroy or de-identify personal information (including images and videos) when it is no longer required. Hard copy records should be shredded, and electronic records permanently deleted from all systems, including backups and offsite storage	R	√			
17. Establishing processes for the safe and secure disposal of broken or unused devices *(refer to Sources)*	R	√			
18. Notifying an individual or family if the service receives personal sensitive and health information about them from another source as soon as practicably possible	R	√			
19. Ensuring that if personal (including photos and videos), sensitive and health information needs to be transferred outside of Victoria, that the individual or family that it applies to has provided consent, or if the recipient of the personal information is subject to a law or binding scheme	R	√			
20. Ensuring the unique identifiers are not adopted, used or disclosed unless lawfully required to *(refer to Attachment 2)*	R	√			
21. Ensuring reasonable steps to destroy personal (including photos and videos), and health information and ensure it is de-identified if the information is no longer required for any purpose as described in *Regulations 177, 183, 184 (refer to Attachment 2)*	R				
22. Complying with the Notifiable Data Breaches Scheme *(refer to Definitions)* which imposes an obligation to notify individual whose personal information (including photos and videos), is in a data breach that is likely to result in serious harm.	R	√			

23. Developing a data breach *(refer to Sources)* response plan that sets out the roles and responsibilities involved in managing a data breach, the steps taken if a data breach occurs *(refer to Sources)* and notifying the *Office of the Australian Information Commission* as appropriate.	R				
24. Promoting awareness and compliance with the Child Safe Standards *(refer to Definitions)*, and disclosing information to promote the wellbeing and safety of a child or group of children by using the Child Information Sharing Scheme, and /or the Family Violence Information Sharing Scheme *(refer to Definitions)*	R	R	R		
25. Abiding by the National Model Code to promote a child safe culture when it comes to taking, sharing and storing images or videos of children in early childhood education and care *(refer to eSafety for Children Policy and Use of Digital Technologies and Online Environment Policy)*	√	√	√		√
26. Ensuring that parents/guardians are informed at the time of enrolment about how photos and videos of children will be used, and that appropriate permission is sought *(refer to Attachment 5)*	R	√	√		√
27. Asking children for permission before taking their photo or video and explain how it will be used. Respecting the child when they say no	√	√	√		√
28. Providing notice to children and parents/guardians when photos/video recordings are going to be taken at the service	√	√	√		√
29. Ensuring that images of children are treated with the same respect as personal information, and as such are protected by privacy laws in the same way	R	R	R	R	R
30. Ensuring the appropriate use of images of children, including being aware of cultural sensitivities and the need for some images to be treated with special care	√	√	√	√	√
31. Being sensitive and respectful to parents/guardians who do not want their child to be photographed or videoed	R	√	√	√	√
32. Being sensitive and respectful of the privacy of other children and parent/guardian in photographs/videos when using and disposing of these photographs/videos	R	√	√		
33. Establishing procedures to be implemented if parents/guardians request that their child's image is not to be taken, published, or recorded, or when a child requests that their photo not be taken	R	√	√		
34. Ensuring that geotagging *(refer to Definitions)* is disabled when taking images or videos of children	R	R			√
35. Including a confidentiality clause relating to appropriate information handling in the agreement or contract between a photographer and the service.	R	√			√
Child Information and Family Violence Sharing Scheme					
36. Ensuring information sharing procedures abide by the *Child Information Sharing Scheme (CISS) Ministerial*	R	R	R		

Guidelines and Family Violence Information Sharing (FVISS) Ministerial Guidelines (refer to Source) and exercising professional judgment when determining whether the threshold for sharing is met, what information to share and with whom to share it *(refer to Attachment 7)*					
37. Identifying which staff should be authorised point of contact in relation to the CISS and the FVISS *(refer to Definitions)*	R	√			
38. Ensuring the authorised point of contact undertakes appropriate training and is aware of their responsibilities under the CISS and FVISS *(refer to Definitions)*	R	√			
39. Being aware of who the point of contact at the service under the CISS and FVISS, and supporting them (if applicable) to complete the threshold test *(refer to Attachment 7)*		R	R		
40. Communicating to staff about their obligations under the Information Sharing Schemes, and ensure they have read this policy	R	√			
41. Providing opportunities for identified ISE staff to undertake the appropriate Information Sharing and MARAM online Learning System training *(refer to Sources)*	R	√			
42. Engaging in training about Information Sharing and MARAM online Learning System training *(refer to Sources)*	√	√	√		
43. Ensuring information sharing procedures are respectful of and have regard to a child's social, individual, and cultural identity, the child's strengths and abilities, and any vulnerability relevant to the child's safety or wellbeing	√	√	√		
44. Ensuring any requests from ISE's are responded to in a timely manner and provide relevant information if the requirements for sharing under CISS or FVISS *(refer to Definitions)* are met *(refer to Attachment 7)*	R	R	R		
45. Promoting a child's cultural safety and recognise the cultural rights and familial and community connections of children who are Aboriginal, Torres Strait Islander or both when sharing information under the CISS and FVISS *(refer to Definitions)*	R	R	R		
46. Giving precedence to the wellbeing and safety of a child or group of children over the right to privacy when sharing information under the CISS and the FVISS *(refer to Definitions)*	R	R	R		
47. Ensuring confidential information is only shared to the extent necessary to promote the wellbeing or safety of a child or group of children, consistent with the best interests of that child or those children	R	R	R		
48. Maintaining record keeping processes that are accurate and complete as set by *Child Wellbeing and Safety (Information Sharing) Regulations* concerning	R	R	R		

both written and verbal sharing of information and or complaints *(refer to Attachment 7)*					
49. Ensuring actions are taken when an ISE becomes aware that information recorded or shared about any person is incorrect, and is corrected in a timely manner	R	R	R		
50. Working collaboratively with services that are authorised and skilled (including those located within The Orange Door) to determine appropriate actions and promote collaborative, respectful practice around parent/guardian and children	R	R	R		
51. Seeking and taking into account the views and wishes of the child and the child's relevant family members, if it is appropriate, safe and reasonable to do so when sharing information under the CISS and the FVISS *(refer to Definitions)*	R	R	R		

PROCEDURES

SHARING INFORMATION AND RECORD KEEPING UNDER THE CHID INFORMATION AND FAMILY VIOLENCE SHARING SCHEME – *REFER TO ATTACHMENT 7*

BACKGROUND AND LEGISLATION

BACKGROUND

Early childhood services are obligated by law, service agreements, and licensing requirements to comply with the privacy and health records legislation when collecting personal and health information about individuals.

The *Health Records Act 2001 (Part 1, 7.1)* and the *Privacy and Data Protection Act 2014 (Vic) (Part 1, 6 (1))* include a clause that overrides the requirements of these Acts if they conflict with other Acts or Regulations already in place. For example, if there is a requirement under the *Education and Care Services National Law Act 2010* or the *Education and Care Services National Regulations 2011* that is inconsistent with the requirements of the privacy legislation, services are required to abide by the *Education and Care Services National Law Act 2010* and the *Education and Care Services National Regulations 2011.*

Adopting the National Model Code is crucial for Early Childhood Education and Care (ECEC) services to ensure the safety and privacy of children. The National Model Code has been designed for voluntary adoption by ECEC services. Under the Code, only service-issued electronic devices should be used for taking photos or recording videos, thereby minimising the risk of unauthorised distribution of images. The Code states that clear guidelines are developed on carrying personal devices for specific essential purposes ensuring that any exceptions are justified and controlled. Additionally, implementing strict controls for storing and retaining images or recordings of children is vital to protect their privacy and prevent misuse of sensitive information. Adhering to these guidelines not only safeguards children but also fosters trust and transparency between ECEC services and families.

In line with the Victorian Government's Roadmap for Reform, Education State reforms and broader child safety initiatives, *Part 6A* of the *Child Wellbeing and Safety Act 2005 (the Act)* was proclaimed in September 2018. The Act established the Child Information Sharing (CIS) Scheme, which enables sharing of confidential information between prescribed entities in a timely and effective manner in order to promote the wellbeing and safety of children. The Act also authorised the development of a web-based platform that will display factual information about children's participation in services known as the Child Link Register (to be rolled out in the early years sector from 2023/2024). The Child Link Register aims to improve child wellbeing and safety

outcomes, monitor and support the participation in government-funded programs and services for children in Victoria.

Alongside the CIS Scheme, the *Family Violence Protection Act 2008* includes the Family Violence Information Sharing (FVIS) Scheme and the Family Violence Multi-Agency Risk Assessment and Management (MARAM) Framework, which enables information to be shared between prescribed entities to assess and manage family violence risk to children and adults. The MARAM Framework can be used by all services including ECEC services that come into contact with individuals and parent/guardian experiencing family violence. The MARAM Framework aims to establish a system-wide shared understanding of family violence. It guides professionals across the continuum of service responses, across the range of presentations and spectrum of risk. It provides information and resources that professionals need to keep victim survivors safe, and to keep perpetrators in view and hold them accountable for their actions.

LEGISLATION AND STANDARDS

Relevant legislation and standards include but are not limited to:

- Associations Incorporation Reform Act 2012 (Vic)
- Child Wellbeing and Safety Act 2005
- Child Wellbeing and Safety (Information Sharing) Amendment Regulations 2020
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011: Regulations 181, 183
- Family Violence Protection Amendment (Information Sharing) Act 2017
- Freedom of Information Act 1982 (Vic)
- Health Records Act 2001 (Vic)
- National Quality Standard, Quality Area 7: Leadership and Service Management
- Privacy Act 1988 (Cth)
- Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Privacy Regulations 2013 (Cth)
- Public Records Act 1973 (Vic)

The most current amendments to listed legislation can be found at:

- Victorian Legislation – Victorian Law Today: www.legislation.vic.gov.au
- Commonwealth Legislation – Federal Register of Legislation: www.legislation.gov.au

DEFINITIONS

The terms defined in this section relate specifically to this policy. For regularly used terms e.g. Approved provider, Nominated supervisor, Notifiable complaints, Serious incidents, Duty of care, etc. refer to the Definitions file of the PolicyWorks catalogue.

Child Information Sharing Scheme (CISS): enables Information Sharing Entities (ISE) *(refer to Definitions)* to share confidential information about any person to promote the wellbeing and/or safety of a child or group of children. The CISS works in conjunction with existing information sharing legislative provisions. All Victorian children from birth to 18 years of age are covered. Unborn children are only captured when there has been a report to Child First or Child Protection. Consent is not required from any person when sharing under CISS. The CISS does not affect reporting obligations created under other legislation, such as mandatory reporting obligations under the *Children, Youth and Parent/guardian Act 2005*.

Child Safe Standards: Promotes the safety of children, prevent child abuse, and ensure organisations have effective processes in place to respond to and report all allegations of child abuse.

Confidential information: For the purposes of this policy, the CISS and FVISS, the health information and identifiers for the *Health Records Act 2001* and the personal information for the *Privacy and Data Protection Act 2014*, including sensitive information (such as a criminal record), and unique identifiers.

Data breach: Unauthorised access or disclosure of personal information, or loss of personal information.

Discloser: In the context of the Schemes, this is defined as sharing confidential information for the purpose of promoting the wellbeing or safety of a child or group of children. In the context of family violence, this is defined as when someone tells another person about violence that they have experienced, perpetrated or witnessed.

Family Violence Information Sharing Scheme (FVISS): enables the sharing of relevant information between authorised organisations to assess or manage risk of family violence.

Freedom of Information Act 1982: Legislation regarding access and correction of information requests.

Geotagging: A piece of electronic data that shows where someone or something is and can, for example, be attached to a photograph or comment on social media.

Health information: Information or opinions about a person's physical or mental health, disability (past, present, or future), health preferences (including future health services), use of health services, bodily donations (e.g., blood or organs), or genetic information.

Health Records Act 2001: State legislation that regulates the management and privacy of health information handled by public and private sector bodies in Victoria.

Identifier/Unique identifier: A symbol or code (usually a number) assigned by an organisation to an individual to distinctively identify that individual while reducing privacy concerns by avoiding the use of the person's name.

Information Sharing Entities (ISE): are authorised to share and request relevant information under the Child Information Sharing Scheme and the Family Violence Information Sharing Scheme (the Schemes) and required to respond to requests from other ISEs. All ISEs are mandated to respond to all requests for information.

Multi-Agency Risk Assessment and Management Framework (MARAM): Sets out the responsibilities of the organisation in identifying, assessing, and managing parent/guardian and guide information sharing under both CIS and FVIS schemes wherever family violence is present.

Notifiable Data Breaches scheme (NDB): a Commonwealth scheme that ensures any organisation or agency covered by the *Privacy Act 1988* notifies affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

Personal information: Information or an opinion about an identified individual or someone who is reasonably identifiable. It can be true or false, verbal, written, photographic, recorded, or unrecorded. Examples include a person's name, address, contact details, date of birth, gender, and IP address.

Privacy and Data Protection Act 2014: State legislation that provides for responsible collection and handling of personal information in the Victorian public sector, including some organisations, such as early childhood services contracted to provide services for government. It provides remedies for interferences with the information privacy of an individual and establishes the Commissioner for Privacy and Data Protection.

Privacy Act 1988: Commonwealth legislation that operates alongside state or territory Acts and makes provision for the collection, holding, use, correction, disclosure, or transfer of personal information. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* introduced on 12 March 2014 has made extensive amendments to the *Privacy Act 1988*. Organisations with a turnover of $3 million per annum or more must comply with these regulations.

Privacy breach: An act or practice that interferes with the privacy of an individual by being contrary to, or inconsistent with, one or more of the Information Privacy Principles *(refer to Attachment 2)* or the new Australian Privacy Principles *(refer to Attachment 7)* or any relevant code of practice.

Public Records Act 1973 (Vic): Legislation regarding the management of public sector documents.

Risk Assessment Entity (RAE): Under FVISS, there is also a subset of specialist ISEs known as Risk Assessment Entities that are able to receive and request information for a family violence assessment purpose. RAEs have specialised skills and authorisation to conduct family violence risk assessment, examples can include but not limited to Victorian Police, child protection, family violence service and some Orange Door services.

Sensitive information: Information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preference or practices, or criminal record. This is also considered to be personal information.

SOURCES AND RELATED POLICIES

SOURCES

- Australia Not-for-profit Law Guide (2025), Privacy Guide: A guide to compliance with privacy laws in Australia*: Privacy-Guide.pdf*
- Australian Signals Directorate*: How to dispose of your device securely*
- Child Care Service Handbook, 2025*: https://www.education.gov.au/early-childhood/resources/child-care-provider-handbook*
- Child Information Sharing Scheme Ministerial Guidelines*: www.vic.gov.au/child-information-sharing-scheme-ministerial-guidelines*
- Family Violence Multi-Agency Risk Assessment and Management Framework: *www.vic.gov.au/family-violence-multi-agency-risk-assessment-and-management*
- Guidelines to the Information Privacy Principles: *www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/*
- Information sharing and Child Link*: www.vic.gov.au/child-information-sharing-scheme-ministerial-guidelines*
- Information Sharing and Family Violence Reforms Toolkit: *www.vic.gov.au/guides-templates-tools-for-information-sharing*
- Information Sharing and MARAM Online Learning System: *ww.training.infosharing.vic.gov.au/login/index.php*
- Information sharing guides, templates and tools*: www.education.vic.gov.au*
- Ministerial Guidelines for the Family Violence Information Sharing Scheme: *www.vic.gov.au/family-violence-information-sharing-scheme*
- National Model Code - Taking images in early childhood education and care: *https://www.acecqa.gov.au/national-model-code-taking-images-early-childhood-education-and-care*
- Office of Australian Information Commissioner, Data breach preparation and response*: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response*
- Office of the Health Complaints Commissioner*: www.hcc.vic.gov.au/*
- Office of the Victorian Information Commissioner, Child information sharing scheme and privacy law in Victoria*: www.ovic.vic.gov.au/wp-content/uploads/2019/01/20190109-Child-information-sharing-scheme-FAQs-1.pdf*
- Office of the Victorian Information Commissioner*: https://ovic.vic.gov.au*

RELATED POLICIES

- Child Safe Environment and Wellbeing
- Code of Conduct

- Compliments and Complaints
- Delivery and Collection of Children
- Enrolment and Orientation
- Use of Digital Technologies and Online Environment
- Staffing
- Inclusion and Equity

EVALUATION

In order to assess whether the values and purposes of the policy have been achieved, the approved provider will:

- regularly seek feedback from everyone affected by the policy regarding its effectiveness
- monitor the implementation, compliance, complaints, and incidents in relation to this policy
- keep the policy up to date with current legislation, research, policy, and best practice
- revise the policy and procedures as part of the service's policy review cycle, or as required
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures, unless a lesser period is necessary due to risk *(Regulation 172 (2))*

ATTACHMENTS

- Attachment 1: Record keeping and privacy laws
- Attachment 2: Privacy Principles in action
- Attachment 3: Letter of acknowledgment and understanding
- Attachment 4: Privacy Statement
- Attachment 5: Permission form for photographs and videos
- Attachment 6: Special permission notice for publications/media
- Attachment 7: Sharing information and record keeping under the Chid Information and Family Violence Sharing Scheme

AUTHORISATION

This policy was adopted by the approved provider of Somerville Kindergarten on August 2025

REVIEW DATE: August 2026