PRIVACY AND CONFIDENTIALITY

QUALITY AREA 7 | ELAA VERSION 1.3

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 Denzil Don Kindergarten
- to ensure compliance with privacy legislation
- for responding to requests for information to promote child wellbeing or safety and/or assess and manage the risk of family violence.

POLICY STATEMENT

VALUES

Denzil Don Kindergarten is committed to:

- responsible and secure collection and handling of personal and health information.
- protecting the privacy of everyone's personal information.
- ensuring individuals are fully informed regarding the collection, storage, use, disclosure, and disposal of their personal 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 staff, students, volunteers, visitors, parents/carers, children, and others attending programs and activities at Denzil Don Kindergarten, including offsite excursions.

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	All staff, including teaching and non-teaching	Parents/carers	Contractors, volunteers, and students
R indicates legislation requirement and should not be deleted.					
Ensuring records and documents are maintained and stored in accordance with *Regulations 181 and 183* of the *Education and Care Services National Regulations 2011*	R	√	√		√
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*	R	√			

Privacy Protection) Act 2012 (Cth), by taking steps to establish and maintain internal practices, procedures, and systems that ensure compliance with privacy legalisations including: • identifying the type of personal, sensitive, and health information to be collected from an individual or a family. • communicating why personal, sensitive, and health information is being collected and how it will be stored, used, disclosed, and managed and providing the Privacy Statement *(refer to Attachment 4)* and 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)* • communicating how an individual or family can complain about any breaches of the privacy legislation and how the service will deal with these complaints.					
Ensuring a copy of this policy is provided to all stakeholders, prominently displayed at the service and/or electronically accessible, up to date, and available on request.	R	√			
Reading the *Privacy and Confidentiality Policy,* including the Privacy Statement *(refer to Attachments 3 & 4 as applicable)*	R	√	√	√	√
Maintaining the management of privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction, or de-identification.	R	√	√		
Protecting personal information from misuse, interference, loss, and unauthorised access, modification, or disclosure.	R	√	√		
Identifying and responding to privacy breaches, handling access and correction requests, and receiving and responding to complaints and inquiries.	R	√			
Providing regular staff training and information on how the privacy legislation applies to them and the service.	R	√			
Ensuring appropriate supervision of staff handling personal, sensitive, and health information regularly.	R	√			
Ensuring personal, sensitive, and health information is only collected by lawful and fair means and is accurate and complete.	R	√	√		
Ensuring parents/carers understand why personal, sensitive, and health information is being collected and how it will be used, disclosed, and managed and are provided with the service Privacy Statement *(refer to Attachment 4)* and all relevant forms.	R	√	√		
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	√	√	√	√
Ensuring secure storage for personal, sensitive, and health information collected by the service, including electronic *(refer to Attachment 2)*	R	√			
Ensuring records are kept in accordance with *Regulation 183*	R	√	√		

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	√			
Ensuring that if personal, sensitive, and health information needs to be transferred outside of Victoria, the individual or family it applies to has provided consent or that the recipient of the personal information is subject to a law or binding scheme.	R	√			
Ensuring unique identifiers are not adopted, used, or disclosed unless lawfully required to *(refer to Attachment 2)*	R	√			
Ensuring reasonable steps to destroy personal 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				
Complying with the Notifiable Data Breaches Scheme *(refer to Definitions)*, which imposes an obligation to notify individuals whose personal information is involved in a data breach likely to result in serious harm.	R	√			
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 breach occurs *(refer to Sources),* and notifying the *Office of the Australian Information Commission* as appropriate.	R				
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.	R	R	R		
Providing notice to children and parents/carers when photos/video recordings are going to be taken at the service	√	√	√		√
Ensuring images of children are treated with the same respect as personal information and, therefore, protected by privacy laws.	R	R	R	R	R
Ensuring the appropriate use of images of children, including being aware of cultural sensitivities and the need for some photos to be treated with special care.	√	√	√	√	√
Being sensitive and respectful to parents/carers who do not want their child to be photographed or videoed.	R	√	√	√	√
Being sensitive and respectful of the privacy of other children and parents/carers in photographs/videos when using and disposing of them.	R	√	√		
Implementing processes for parents/carers requesting that their child's photo is not taken or a child says that they don't want their photo taken	R	√	√		
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					
Ensuring information sharing procedures abide by the *Child Information Sharing Scheme (CISS) Ministerial 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,	R	R	R		

what information to share and with whom to share it *(refer to Attachment 7)*					
Nominating a staff member as an authorised point of contact in relation to the CISS and the FVISS *(refer to Definitions)*	R	√			
Ensuring the authorised point of contact undertakes appropriate training and is aware of their responsibilities under the CISS and FVISS *(refer to Definitions)*	R	√			
Being aware of the point of contact at the service under the CISS and FVISS and supporting them to complete the threshold test *(refer to Attachment 7)*		R	R		
Communicating staff obligations under the Information Sharing Schemes and ensuring they read this policy.	R	√			
Providing opportunities for identified ISE staff to undertake the appropriate Information Sharing and MARAM online Learning System training *(refer to Sources)*	R	√			
Engaging in training about Information Sharing and MARAM online Learning System training *(refer to Sources)*	√	√	√		
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.	√	√	√		
Ensuring requests from ISEs are responded to promptly 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		
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		
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		
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(ren).	R	R	R		
Maintaining record-keeping processes that meet the *Child Wellbeing and Safety (Information Sharing) Regulations* concerning the sharing of information and or complaints *(refer to Attachment 7)*	R	R	R		
Ensuring actions are taken when an ISE becomes aware that information recorded or shared about a person is incorrect and correcting it promptly	R	R	R		
Working collaboratively with services authorised and skilled to determine appropriate actions and promote collaborative, respectful practice around parents/carers and children	R	R	R		
Seeking and considering the views and wishes of the child and their relevant family members, if it is appropriate, safe, and	R	R	R		

reasonable to do so when sharing information under the CISS and the FVISS *(refer to Definitions)*					

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.*

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 the sharing of confidential information between prescribed entities in a timely and effective manner to promote the wellbeing and safety of children. The Act also authorised the development of a web-based platform that will display information about children's participation in services known as the Child Link Register (to be rolled out in the early years from 2024). The Child Link Register aims to improve child wellbeing and safety outcomes and 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 that come into contact with individuals and parents/carers 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, 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. Refer to the definitions file on the kindergarten website for regularly used terms.

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 are covered. Unborn children are only covered when a report to Child First or Child Protection has occurred. 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, prevents child abuse, and ensures organisations have effective processes in place to respond to and report all allegations of child abuse.

Confidential information: (for this policy) 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, disclosure, or loss of personal information.

Disclosure: in the context of the Schemes, is defined as sharing confidential information to promote the wellbeing or safety of a child or group of children. In context of family violence it is when someone tells another person about the violence 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 concerning the access and correction of information requests.

Health information: any information or an opinion about an individual's physical, mental, or psychological health or ability.

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 assigned by an organisation to an individual to distinctively identify that individual while reducing privacy concerns by avoiding using their 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 organisation's responsibilities in identifying, assessing, and managing parent/carer and guides 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: Recorded information (including images) or opinion, whether true or not, about a living individual whose identity can reasonably be ascertained.

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 a subset of specialist ISEs known as Risk Assessment Entities that can receive and request information for a family violence assessment purpose. RAEs have specialised skills and authorisation to conduct family violence risk assessment, and include the 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

- *Childcare Service Handbook Version 2, 2019*
- *Child Information Sharing Scheme Ministerial Guidelines*
- Ministerial Guidelines for the Family Violence Information Sharing Scheme
- *Guidelines to the Information Privacy Principles*
- ELAA Early Childhood Management Manual
- Office of the Health Complaints Commissioner
- *Australia Not-for-profit Law Guide (2017), Privacy Guide: A guide to compliance with privacy laws in Australia*
- *Office of Australian Information Commissioner, Data breach preparation and response*
- Office of the Victorian Information Commissioner
- Information Sharing and Family Violence Reforms Contextualised Guidance
- Information Sharing and Family Violence Reforms Toolkit
- Office of the Victorian Information Commissioner, Child information sharing scheme and privacy law in Victoria
- Family Violence Multi-Agency Risk Assessment and Management Framework
- Information Sharing and MARAM Online Learning System

RELATED POLICIES

- Child Safe Environment and Wellbeing
- Code of Conduct

- Compliments and Complaints
- Delivery and Collection of Children
- Enrolment and Orientation
- Information, Communication and Technology
- Staffing
- Inclusion and Equity

EVALUATION

To assess whether the values and purposes of the policy have been achieved, the service will:

- Regularly seek feedback regarding its effectiveness from everyone affected by the policy.
- 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.
- Notify all affected by this policy at least 14 days before making any significant changes to it 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: Sharing information and record keeping under the Chid Information and Family Violence Sharing Scheme

AUTHORISATION

This policy was adopted by the approved provider of Denzil Don Kindergarten on 28/12/2023.

REVIEW DATE: 28 / DECEMBER / 2025

ATTACHMENT 1. RECORD KEEPING AND PRIVACY LAWS

Services must ensure their processes for collecting, storing, using, disclosing, and disposing of personal, sensitive, and health information meet the requirements of the appropriate privacy legislation and the *Health Records Act 2001*.

The following are examples of records impacted by the privacy legislation:

- **Enrolment records:** *Regulations 160, 161, and 162 of the Education and Care Services National Regulations 2011 detail the information that must be kept on a child's enrolment record, including personal details about the child and the child's family, parenting orders,* and medical conditions. This information is classified as personal, sensitive, and health information *(refer to Definitions)* and must be stored securely and disposed of appropriately.
- **Attendance records**: *Regulation 158* of the *Education and Care Services National Regulations 2011* requires details of the date, child's full name, times of arrival and departure, and signature of the person delivering and collecting the child or educator to be recorded in an attendance record kept at the service.
- **Medication records and incident, injury, trauma, and illness records:** *Regulations 87 and 92* of the *Education and Care Services National Regulations 2011* require the service to retain incident, injury, trauma, and illness records and medication records that contain personal and health information about the child.
- **Handling and storing information:** confidential information held by the service mustn't be accessible to unauthorised staff or other persons. When confidential information is required to be taken off-site (e.g., on excursions), consideration must be given to how this is transported and stored securely.
- **Electronic records:** electronic records containing personal, sensitive or health information are stored with password protection and are only accessible by authorised personnel *(refer to the Information Technology Policy).*
- **Forms:** enrolment forms and any other forms used to collect personal, sensitive or health information should have the service's Privacy Statement attached *(refer to Attachment 4)*.
- **Collecting information for which there is no immediate use:** services should not collect information without immediate use.

ATTACHMENT 2. PRIVACY PRINCIPLES IN ACTION

Your organisation may have to comply with more than one set of privacy obligations listed below. For example, an organisation that has a contract with a Victorian government agency may need to comply with the Australian Privacy Principles [AAP] *(Privacy Act, 1988)* as well as the Information Privacy Principles [IPP] *(Privacy and Data Protection Act, 2014)*, and the Health Privacy Principles [HPP] *(Health Records Act, 2001)*.

The Australian Privacy Principles

The APPs are legal obligations under federal Privacy Laws. They apply to every Australian organisation and federal government agency that meets the qualifying criteria below:

- it has an annual turnover of more than $3 million.
- it provides a health service (which is broadly defined) to a person (even if the organisation's primary activity is not providing that health service)
- it trades in personal information (for example, buying or selling a mailing list)
- it is a contracted service provider under a Commonwealth contract (for example, an aged care provider or a disability services provider under a Commonwealth agreement)
- it is a credit reporting body.
- it operates a residential tenancy database.
- it is a reporting entity for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act)
- it is an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009 (Cth)
- it is a business that conducts protection action ballots.
- it is a business prescribed by the Privacy Regulation 2013
- it is related to a body corporate (for example, a subsidiary) that meets any of the above criteria (even if your not-for-profit itself does not) or
- it has opted into the Privacy Act (choosing to comply despite not meeting any of the above criteria

The Information Privacy Principles

The IPPs are relevant for all Victorian public sector organisations and some private or community sector organisations, which carry out functions under a State contract with a Victorian public sector organisation.

A State contract means a contract between an organisation (e.g. the Department of Education) and a Contracted Service Provider [CSP] (e.g. an Approved Provider) under which the CSP provides services for the organisation (e.g. a funded Kindergarten Program).

The Health Privacy Principles

Victoria has specific Health Privacy Laws that provide a higher standard of protection for certain health information. Early Childhood Education and Care services collect, hold, and use health information and must follow the HPP under the Health Records Act of *2001*.

Principles in Action

Organisations must ensure their policy and procedures are consistent with all the Privacy Laws that apply to their organisation. If you're not sure, you should get legal advice.

The Child Information Sharing Scheme and Family Violence Information Sharing Scheme makes certain modifications to the Information Privacy Principles and the Health Privacy Principles to ensure that the scheme can operate as intended.

The table below is a reference tool that identifies how all three legislations can work together and what it may look like in practice.

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
APP 1 – Open and transparent management of personal information	IPP 5: Openness	Principle 5 Openness	Denzil Don Kindergarten (the service) has an up-to-date *Privacy and Confidentiality policy* that sets out how we collect, use, disclose, and store personal and health information. Stakeholders have access to this policy at any time upon request.
APP 2 – Anonymity and pseudonymity	IPP 8: Anonymity	Principle 8 Anonymity	Wherever it is lawful and practicable, individuals and parents/carers will have the option of not identifying themselves when entering transactions with the service (i.e., surveys, feedback, etc).
APP 3 Collection of solicited personal information and APP 4 – Dealing with unsolicited personal information	IPP 1: Collection IPP 10: Sensitive information	Principle 1 Collection	The service will only collect the personal, sensitive, and health information needed and for which there is a purpose that is legitimate and related to the service's functions, activities, and/or obligations. Personal, sensitive, and health information about children and parents/carers, either in relation to themselves or a child enrolled at the service, will generally be collected via forms completed by parents/carers. This can include but is not limited to Enrolment Records, Medical Management Plans, Risk Minimisation Plans, Communication Plans, Attendance Records, Staff Records, and visitor logbooks. Other information may be collected from job applications, interviews, and phone calls. Individuals from whom personal information is collected will be provided a copy of the service's *Privacy Statement (refer to Attachment 4).* When the service receives personal information *(refer to Definitions)* from a source other than directly from the individual or the parents/carers of the child concerned, the person receiving the information will notify the individual or the parents/carers of the child to whom the information relates. The service will advise the individual on their right to share or not share this information with the source. Sensitive information *(refer to Definitions)* will be collected only to enable the service to provide for the education and care of the child attending the service. CISS & FVISS: Information-sharing entities are not obliged to collect personal or health information about an individual directly from that person if they are collecting the information from another information-sharing entity under the scheme. If an information-sharing entity collects personal or health information about a person from another information-sharing entity under the scheme, it will not be obliged to take reasonable steps to notify that person that their information has been collected if doing so would be contrary to the wellbeing or safety of a child.

<table>
<tr><td></td><td></td><td></td><td>Information-sharing entities will not be obliged to obtain consent from any person before collecting information under the scheme, including ‘sensitive information’ if they are sharing in accordance with the scheme.</td></tr>
<tr><td>APP 5 – Notification of the collection of personal information and APP 6 – Use or disclosure of personal information</td><td>IPP 2: Use and disclosure</td><td>Principle 2 Use and Disclose</td><td>Whenever personal, sensitive, or health information is collected, the service will take reasonable steps to ensure individuals or parents/carers understand why this information is being collected, used, disclosed, and stored. Individuals or parents/carers will be informed of the following:

• the service contact details.
• the facts, purpose, and circumstances of why personal, sensitive, and health information is being collected.
• what information is required by authorised law.
• the consequences if personal information is not collected.
• the service's usual disclosures of personal information; if applicable
• the service Privacy and Confidentiality Policy.

The following table identifies the personal, sensitive, and health information that will be collected by the service, the primary purpose for its collection, and some examples of how this information will be used.

<table>
<tr><td>Personal, sensitive, and health information collected in relation to:</td><td>The primary purpose of collection:</td><td>Examples of how the personal and health (including sensitive) information will be used:</td></tr>
<tr><td>Children and parents/carers</td><td>• To the provision of education and care for children attending the service.</td><td>• Day-to-day administration and delivery of service
• Provision of a place for their child in the services
• Looking after children’s educational, care, and safety needs
• For parent/carer correspondence regarding their child’s attendance
• To satisfy the service’s legal obligations and to allow it to discharge its duty of care.</td></tr>
</table>
</td></tr>
</table>

			The Committee of Management • For the management of the service • For communication with and between the Approved Provider, other Committee/Board members, employees, and members of the association • To satisfy the service's legal obligations Job applicants, employees, contractors, volunteers, and students • To assess and (if necessary) engage the applicant, employees, contractor, volunteers, or students. • To administer employment, contract, or placement • Administering an individual's employment contract or placement • Ensuring the health and safety of the individual • Insurance • Promoting the service through the service's website The service may disclose personal and/or health information held about an individual to: • government departments or agencies, as part of its legal and funding obligations • local government authorities, in relation to enrolment details for planning purposes • organisations providing services related to staff entitlements and employment. • insurance providers, in relation to specific claims or for obtaining cover. • law enforcement agencies. • health organisations and/or parents/carers in circumstances where the person requires urgent medical assistance and is incapable of giving permission. • anyone to whom the individual authorises the service to disclose information. Sensitive information *(refer to Definitions)* will be used and disclosed only for the purpose for which it was collected unless the individual agrees otherwise or where the use or disclosure of the information is allowed by law.
APP 7 – Direct marketing	N/A		N/A
APP 8 – Cross-boarder disclosure of	IPP 9: Transborder data flows	Principle 9 Transborder Data Flows	The service will only transfer personal health information outside Victoria in certain circumstances.

personal information			
APP 9 – Adoption, use, or disclosure of government-related identifiers	IPP 7: Unique identifiers	Principle 7 Identifiers	Unless an exception applies, the service will not adopt, use, or disclose a government-related identifier. The service will collect information on the following identifiers *(refer to Definitions),* including but not limited to: • information required to access the *Kindergarten Fee Subsidy* for eligible parents/carers. • tax file number for all employees. • Medicare number: for medical emergencies.
APP 10 – Quality of personal information	IPP 3 - Data quality	Principle 3 Data quality	The service will take reasonable steps to ensure that the personal and health information it collects is accurate, up-to-date, and complete, as this Privacy and Confidentiality Policy outlines. The service will ensure any updated or new personal and/or health information is promptly added to existing records and will send timely reminders to individuals or parents/carers to update their personal and/or health information to ensure records are always up to date.
APP 11 – Security of personal information	IPP 4 - Data security	Principle 4 Data Security and Data Retention	The service takes active measures to ensure the security of personal, sensitive and health information it holds, and takes reasonable steps to protect the stored information from misuse, interference, and loss, as well as unauthorised access, modification, or disclosure *(refer to Privacy and Confidently policy)*. The service also takes reasonable steps to destroy personal and health information and ensure it is de-identified if it is no longer needed for any purpose, as described in *Regulations 177, 183, 184.* In the disposal of personal, sensitive, and/or health information, those with authorised access to the information will ensure that it is destroyed so that the information is no longer accessible. The service will ensure that in relation to personal, sensitive, and health information: • access will be limited to authorised staff, the Approved Provider, or other individuals who require this information to fulfill their responsibilities and duties. • information will not be left in areas that allow unauthorised access to that information. • all materials will be stored securely, • digital records will be stored safely and secured with a password. • there is security in the transmission of the information via email, phone/text messages, as below: ○ emails will only be sent to a person authorised to receive the information. ○ phone – limited and necessary personal information will be provided to persons authorised to receive that information over the telephone. • transfer of information interstate and overseas will only occur with the permission of the person concerned or their parents/carers.

APP 12 – Access to personal information and APP 13 – Correction of personal information	IPP 6 - Access and correction	Principle 6 Access and Correction	Individuals or parents/carers have the right to seek access to their personal information and to make corrections to it if necessary. Upon request, the service will promptly grant an individual, parent/carer access to personal or health information. The service must be satisfied through identification verification, that a request for personal or health information is granted. A person may seek access to view or update their personal or health information by contacting the Centre Coordinator or Nominated Supervisor. Personal information may be accessed by viewing the information, taking notes, and/or obtaining copies. Individuals requiring access to or updating (including correcting) personal information should nominate the type of access required and specify, if possible, what information is required. The Centre Coordinator will endeavour to respond to this request within 45 days of receiving it. The service will provide access in line with the privacy legislation. If the requested information cannot be provided, the reasons for denying access will be given to the person requesting the information in writing. In accordance with the legislation, the service reserves the right to charge for information provided to cover the costs involved in providing that information. There are some exceptions set out in the *Privacy and Data Protection Act 2014,* where access may be denied in part or total: • the request is frivolous or vexatious. • providing access would have an unreasonable impact on the privacy of other individuals. • providing access would pose a serious threat to the life or health of any person. • the service is involved in detecting, investigating, or remedying serious improper conduct, and providing access would prejudice that.
N/A	Principle 10 Transfer or closure of the practice of a health service provider		N/A
N/A	Principle 11 Making information available to another health service provider		N/A

ATTACHMENT 3. ACKNOWLEDGEMENT AND UNDERSTANDING FOR EMPLOYEES

Denzil Don Kindergarten's *Privacy and Confidentiality Policy* outlines how the service will meet the requirements of the *Victorian Health Records Act 2001* and the *Privacy and Data Protection Act 2014 (Vic)* (or where applicable, the *Privacy Act 1988 (Cth)*), The Child Information Sharing Scheme under Part 6A of the *Child Wellbeing and Safety Act 2005* and the Family Violence Information Sharing Scheme under Part 5A of the *Family Violence Protection Act 2008* in relation to both personal, sensitive and health information.

Employees have an important role in assisting the service to comply with the privacy legislation requirements by ensuring they understand and implement the *Privacy and Confidentiality Policy*. Employees need to ensure they are aware of their responsibilities in relation to the collection, storage, use, disclosure, and disposal of personal and health information and the requirements for the handling of personal and health information, as set out in this policy.

(TO BE SIGNED DIGITALLY) Acknowledgement of reading the *Privacy and Confidentiality Policy*

I (insert name) have read the service's *Privacy and Confidentiality Policy* and understand my responsibilities in relation to the collection, storage, use, disclosure, and disposal of personal and health information and the requirements for the handling of personal and health information, as set out in this policy.

Signature: _____

Date: _____

ATTACHMENT 4. PRIVACY STATEMENT

We know your privacy is important.

Denzil Don Kindergarten's *Privacy and Confidentiality Policy* explains how we collect, use, disclose, manage, and transfer personal information, including health information. All policies are available on our website: https://denzildonkinder.org.au/policies/

To ensure ongoing funding and licensing, our service must comply with privacy legislation requirements concerning collecting and using personal information. If we need to collect health information, our procedures are subject to the *Health Records Act 2001*.

The Child Information and Family Violence Information Sharing Scheme allows Early Childhood Services to freely request and share relevant information with Information Sharing Entities to support a child or group of children's wellbeing and safety when the threshold test has been met.

Purpose for which information is collected

The reasons we generally collect personal information are detailed below.

Personal information and health information collected in relation to:	**The primary purpose for which information will be used:**
Children and parent/carer	• To provide education and care of children attending the service • To manage and administer the service as required
Committee of Management	• For the management of the service • To comply with relevant legislation requirements
Job applicants, employees, contractors, volunteers, and students	• To assess and (if necessary) to engage employees, contractors, volunteers, or students. • To administer employment contracts or placement of students and volunteers

Please note that under relevant privacy legislation, other uses and disclosures of personal information may be permitted as set out in that legislation.

Disclosure of personal information, including sensitive and health information

Some personal information, including health information, held about an individual may be disclosed to:

- government departments or agencies, as part of our legal and funding obligations
- local government authorities, for planning purposes
- organisations providing services related to employee entitlements and employment.
- insurance providers, in relation to specific claims or for obtaining cover.
- law enforcement agencies
- health organisations and/or parent/carer in circumstances where the person requires urgent medical assistance and is incapable of giving permission.
- anyone to whom the individual authorises us to disclose information.
- information sharing entities to support a child and a group of children's wellbeing and safety.

Laws that require us to collect specific information

The Education and Care Services National Law Act 2010 and the *Education and Care Services National Regulations 2011, Associations Incorporation Reform Act 2012 (Vic),* and employment-related laws and agreements require us to collect specific information about individuals from time-to-time. Failure to provide the necessary information could affect:

- a child's enrolment at the service

- a person's employment with the service
- the ability to function as an incorporated association.

Access to information

Individuals about whom we hold personal, sensitive, or health information can gain access to this information in accordance with applicable legislation. The procedure for doing this is set out in our *Privacy and Confidentiality Policy*, which is available on request.

For information on the *Privacy and Confidentiality Policy*, please refer to the copy available at the service or contact the Centre Coordinator.

ATTACHMENT 5. SHARING INFORMATION UNDER CISS AND FVISS

Applying the threshold test under CISS

The threshold test requirements must be met before sharing information with other Information Sharing Entities (ISE).

The requirements for sharing are different depending on the purpose of the sharing. If sharing is for both purposes (Child wellbeing or safety and/or family violence), you must meet the requirements of each scheme.

Although child wellbeing and safety takes precedence over an individual's privacy, privacy must still be protected through careful and selective information sharing.

Threshold requirements for the Child Information Sharing Scheme:

1	The information-sharing entity is requesting or disclosing confidential information about any person to promote the wellbeing or safety of a child or group of children and
2	The **disclosing** information-sharing entity reasonably believes that sharing the confidential information may assist the receiving information-sharing entity in carrying out one or more of the following activities: • make a decision, an assessment, or a plan relating to a child or group of children. • initiate or conduct an investigation relating to a child or group of children. • provide a service relating to a child or group of children, • manage any risk to a child or group of children, and
3	The information being **disclosed** or **requested** is not known to be 'excluded information' under Part 6Aof the Child Wellbeing and Safety Act (and is not restricted from sharing by another law), information that could: • endanger a person's life or result in physical injury. • prejudice a police investigation or interfere with the enforcement or administration of the law; prejudice a coronial inquest; prejudice a fair trial of a person. • be legally privileged. • reveal confidential police sources. • contravene a court order. • be contrary to the public interest. • information sharing would contravene another law.

Requirements for the Family Violence Information Sharing Scheme:

1	**The purpose of sharing is to assess family violence risk OR protect victim-survivors from family violence risk.** There are two purposes for which information can be shared between ISEs: • Family violence assessment purpose: the purpose of establishing or assessing the risk of a person committing family violence or being the subject of family violence. This would include: ○ establishing family violence risk ○ assessing the risk to the victim survivor ○ correctly identifying the perpetrator.

	Family violence protection purpose: once family violence risk is established, manage the risk to the victim-survivor. This includes information sharing to support ongoing risk assessment.
2	**The applicable consent requirements are met.** Is the consent required when a child is at risk of family violence? • Consent is not required from any person to share information relevant to assessing or managing family violence risk to a child. However, you should seek the child's views and non-violent family members where it is safe, reasonable, and appropriate. • In situations where an adolescent is using family violence against an adult family member, you may need the consent of the adult victim survivor to share their information.
3	**The information is not excluded information.** Excluded information is information that could: • endanger a person's life or result in physical injury. • prejudice a police investigation or interfere with the enforcement or administration of the law; prejudice a coronial inquest; prejudice a fair trial of a person being legally privileged. • reveal confidential police sources. • contravene a court order. • be contrary to the public interest. • information sharing would contravene another law.

Requesting another Information Sharing Entity

Before disclosing information under the Child Information Sharing Scheme and/or Family Violence Information Sharing Scheme, it is important that information sharing entities take reasonable care to verify the identity of the professional or service and ensure that they are an information sharing entity.

- The ISE list is a searchable database that can be used to identify organisation and services prescribed under the CISS and FIVSS
- Before making a request, check to see if the organisation is a prescribed entity via the Access the ISE list
- Refer to the Information Sharing Entity List Uses Guide on how to navigate the database.
- ISEs should promptly respond to requests for information, including when they are declining to provide information in response to the request.
- If an ISE is declining a request from another ISE, they must provide written reasons for doing so.

Making a request or receiving a request under the Child Information Sharing Scheme

An ISE may request information when it meets the first and third parts of the threshold. That is, the information being requested is:

- to promote the wellbeing or safety of a child or group of children
- not excluded information under the Child Information Sharing Scheme to their knowledge.

ISE should use professional judgement to determine which organisation/service to request information from by considering the following:

- the activity the requesting information-sharing entity is seeking to undertake and the type of information that may assist them.
- the roles and responsibilities of other information-sharing entities and the information they will likely hold.
- the currency and relevance of the information other information-sharing entities are likely to hold.

The ISE requesting the information should provide sufficient detail to enable the responding ISE to decide whether all three parts of the threshold have been met to assist them to:

- identify relevant information to respond to the request.
- form an opinion about whether the information may be disclosed under the CISS (meets the threshold).

When making a request, an ISE may disclose any confidential information that may assist the responding ISE to:

- identify the information they hold that is relevant to the request.
- form an opinion on whether the information may be disclosed under the scheme.

If the legal requirements (or threshold) of the scheme are met, an ISE:

- **may** make requests for information to another ISE.
- **must** disclose relevant information to another ISE if requested.
- **may** disclose information voluntarily (proactively) to other ISEs.

ISEs will use their expertise and exercise their professional judgement to identify the following:

- the range of needs and risks that impact a child's life to decide whether the threshold is met.
- what and how much information to share
- who to share with to support improved service delivery/promote the wellbeing or safety of the child or children.

Making a request or receiving a request under the Family Violence Information Sharing Scheme

Under Part 5A of the *Family Violence Protection Act 2008* (FVPA), ISEs may request or share information with other ISEs about a person relevant to assessing or managing a family violence risk. The information may relate to a victim survivor (adult or child), alleged perpetrator/perpetrator, or third party.

Only information that is **relevant** to assessing or managing a risk of family violence can be shared under the Scheme. In determining relevant information, practitioners should use their professional judgement and refer to the *Family Violence Policy*.

Where an ISE receives a request, it **must** share that information, verbally or in writing, provided it meets the Scheme's requirements. The onus is on the ISE sharing information to ensure that they are disclosing information about a person in accordance with the law. There is no restriction on an ISE making a request.

If there is no existing relationship with the ISE the information is being requested from, verification may need to take place (e.g. by sending an email with the entity's official account).

There are **two purposes** for which ISEs can share information with each other under the FVPA, Part 5A:

a. for family violence assessment purposes

- Only prescribed risk assessment entities (RSE) (see Definition) are entitled to make requests and receive information for a family violence assessment purpose, which focuses on identifying who the 'actual' perpetrator and victim-survivor are and establishing the level of risk the perpetrator poses to the victim survivor.

OR

b. for family violence protection purposes

- Any prescribed ISE is permitted to request and receive information for the purpose of family violence protection. The focus at this stage is on managing risk of the perpetrator committing family violence or the victim survivor being subjected to family violence. This could include information sharing as part of ongoing risk assessment.

Once it has been established which purpose the information is to be exchanged, ensure that:

- sufficient information is provided to the ISE to help them identify what information they hold that might be relevant and whether they should disclose it.
- the purpose of the information is clearly identified, and why it is believed the information is relevant.
- precedence is given to a victim survivor's right to be safe from family violence when discussing relevant information.
- record keeping is complete, including the name of the service that was contacted, the name of the ISE, and the information that was disclosed.
- any risk assessment or safety plan is documented due to the information sharing.
- information is used only for a purpose permitted by law.

- if an information request is refused, record this refusal in writing and keep this refusal on file.

Sharing information for risk assessment

Once a reasonable belief has been established that family violence risk is present and the identity of the perpetrator or victim survivor is clear (e.g., the victim-survivor has identified the perpetrator), this would enable any ISE to make referrals for specialist services or professionals to complete a comprehensive family violence risk assessment. Some of these specialist services are prescribed as Risk Assessment Entities (RAEs) *(refer to Table 1).*

ISEs can share relevant information proactively or on request with RAEs for risk assessment purposes. That is, to:

- confirm whether family violence is occurring.
- enable RAEs to assess the level of risk the perpetrator poses to the victim survivor.
- correctly identify the perpetrator who is using family violence.

Family violence risk assessment is an ongoing process and is required at different points in time from different service perspectives. Education and care services will have a role in working collaboratively with other services to contribute to ongoing risk assessment and management of family violence.

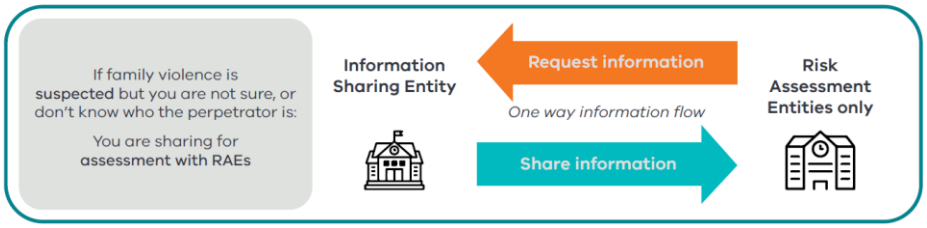

Figure 1: Overview of activities when sharing information for risk assessment

Victoria State Government, 2021. *Information Sharing and Family Violence Reforms Contextualised Guidance*. Melbourne, p.38.

ISEs can only share information with other ISEs that are not RAEs. Request information from RAEs once family violence risk is established and the identity of the perpetrator and victim-survivors are known. This is to prevent sharing that might escalate risk to a child or family member.

Sharing for risk management (protection):

Once family violence is established, ISEs can share proactively with other ISEs and request information, including from RAEs, if they reasonably believe sharing is necessary to:

- remove, reduce, or prevent family violence risk.
- understand how risk is changing over time.
- inform ongoing risk assessment.

This opens a two-way flow of information that enables ISEs to form a complete picture of risk and collaborate to support children and parent/guardian experiencing family violence.

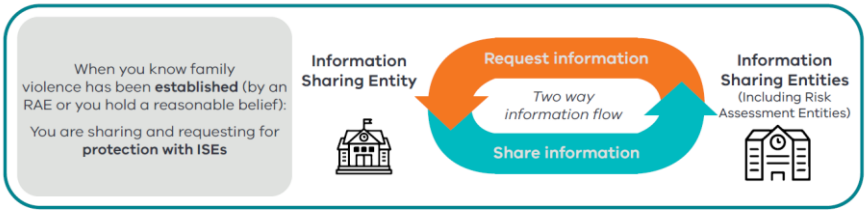

Figure 2: Overview of activities when sharing information for risk management (protection)

Victoria State Government, 2021. *Information Sharing and Family Violence Reforms Contextualised Guidance*. Melbourne, p.39.

When making a request, ensure you are speaking with someone suitably trained to use Part 5A of the Family *Violence Protection Act 2008* (FVPA).

Table 1

Information Sharing Entities that are also Risk Assessment Entities	
▪ State-funded specialist family violence services (including refuges, Men's Behaviour Change Programs, family violence counselling, and therapeutic programs) ▪ Risk Assessment and Management Panel (RAMP) members (including those services that would not otherwise be prescribed but only when participating in a RAMP) ▪ State-funded sexual assault services	▪ Child Protection ▪ Child FIRST services (excluding broader family services) ▪ Victims Support Agency (including Victim Assistance Programs and Victims of Crime Helpline) ▪ Victoria Police ▪ The Orange Door services.
Information Sharing Entities	
▪ Magistrates' Court of Victoria officials ▪ Children's Court of Victoria officials ▪ Corrections Victoria and Corrections-funded services ▪ Adult Parole Board ▪ Youth Justice (including the Secretariat to the Youth Parole Board) and Youth Justice funded services ▪ Multi-Agency Panels to Prevent Youth Offending ▪ Justice Health and funded services ▪ State-funded sexually abusive behaviour treatment services ▪ State-funded perpetrator intervention trials ▪ Registered community-based child and family services	▪ Maternal and Child Health ▪ Registered out-of-home care services ▪ Department of Parent/carer, Fairness and Housing ▪ State-funded homelessness accommodation or homelessness support services providing access point, outreach, or accommodation services ▪ Designated mental health services ▪ State-funded alcohol and other drug services ▪ Tenancy Advice and Advocacy Program ▪ State-funded financial counselling services ▪ Commission for Children and Young People ▪ Disability Services Commissioner.

Record keeping

ISEs have specific record-keeping obligations under the FVISS and the CISS. ISEs can choose how they will meet their record-keeping obligations, which might include written or online case notes, specific record-keeping forms, or IT solutions, and are in line with the *Privacy and Data Protection Act 2014 (Vic)* and, where applicable, the Australia Privacy Principles obligations.

When an ISE receives a request to share information, they must record:

- the ISE that requested the information
- the date of the request
- the information that was requested
- if refusing a request, the request and why it was refused.

When an ISE shares information (either proactively or on request), they should:

- know and record what scheme they are sharing under (FVISS, CISS, or both)
- know and record whom information is being shared about.
- record how the threshold for sharing was met.
- relevant risk assessments or safety plans that have been prepared for a person at risk of family violence.

Documentation is also required if sharing about:

- adult victim survivors of family violence or third parties under FVISS (where a child is at risk)
- a child's parent under CISS
- child victim survivors of family violence
- any child to promote their wellbeing or safety.
- whether their views were sought about sharing their information
- if their views were not sought, record the reason why.
- if they were informed that their information was shared
- whether information was shared with consent and whether the consent was written, verbal, or implied.

- if the information was shared without consent, record why.
- if the information was shared without consent, record if the person was informed that their information was shared without consent.

Handling information sharing and risk assessment complaints under the CISS and FVISS

Types of complaints

ISEs may receive complaints from:

1. Individuals in relation to privacy breaches, for example, the ISE has:
- misidentified an adult victim survivor as a perpetrator and shared information about them without consent
- shared information that is not relevant to the purpose for which it was shared.
2. Individuals in relation to any other conduct under the Schemes, for example, the ISE has:
- not sought the views of a child and/or relevant family member, and the complainant believes it was reasonable, safe, and appropriate to do so
- in the view of the complainant, failed to foster positive relationships between a child and significant people in the child's life, in the way they applied the Schemes.
3. Other ISEs in relation to how the ISE shares information under the Schemes. For example, an ISE may make a complaint about:
- another ISE refusing to share relevant information that should be shared
- the timeliness of responses.

Complaints record keeping

The following information must be recorded if a complaint is received under the Schemes:

- date the complaint was made and received.
- nature of the complaint
- action taken to resolve the complaint.
- action taken to lessen or prevent the issue from recurring.
- time taken to resolve the complaint.
- if the complaint was not resolved, further action was taken.

Note: accepted standard practice is that a response should be provided within 30 days of receiving the complaint. All complaints must be handled according to the *Privacy and Data Protection Act 2014 (Vic)* and, where applicable, the Australia Privacy Principles.