PRIVACY AND CONFIDENTIALITY POLICY

QUALITY AREA 7 (MANDATORY)

Version 1.5

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 St Francis of Assisi OSHC
- 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

St Francis of Assisi OSHC is committed to:

- responsible and secure collection and handling of personal 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 information (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, educators, staff, students, volunteers, parents/guardians, children, and others attending the programs and activities of, including during offsite excursions and activities.

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Educators and all other staff	Parents/guardians	Contractors, volunteers and students
Ensuring all records and documents (including images and videos) 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 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**	√			
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**	√			
Reading and acknowledging they have read 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, as well as 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 that personal, sensitive, and health information is only collected by lawful and fair means, and is accurate and complete	**R**	√	√		
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**	√	√		
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**	√	√	√	√
Providing adequate and appropriate secure storage for personal, (including photos and images), sensitive, and health information collected by the service, including electronic storage *(refer to Attachment 2)*	**R**	√			
Ensuring that records and documents 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 (including photos and images), 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**	√			
Ensuring the unique identifiers, are not adopted, used or disclosed unless lawfully required to *(refer to Attachment 2)*	**R**	√			
Ensuring reasonable steps to destroy personal (photos and images) 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 individual whose personal information (includes photos and images) is in a data breach that is 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 data breach occurs *(refer to Sources)* and notifying the *Office of the Australian Information Commission* as appropriate. *(Refer to Attachment 8)*	**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 by using the Child Information Sharing Scheme, and/or the Family Violence Information Sharing Scheme *(refer to Definitions)*	**R**	**R**	**R**		
Adopting 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 e-Safety for Children Policy and Information Communication and Technology Policy)*	√	√	√		√
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**	√	√		√
Ensuring that images of children are treated with the same respect as personal information, and as such as protected by privacy laws in the same way	**R**	**R**	**R**	**R**	**R**
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	√	√	√	√	√
Being sensitive and respectful to parents/guardians who do not want their child to be photographed or videoed	**R**	√	√	√	√
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**	√	√		
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**	√	√		
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 Sources)* 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)*	**R**	R	R		
Identifying which staff should be 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 who the point of contact at the service under the CISS and FIVSS, and supporting them (if applicable) to complete the threshold test *(refer to Attachment 7)*		**R**	**R**		

Communicating to staff about their obligations under the Information Sharing Schemes, and ensure they have read this policy	**R**	√			
Providing opportunities for identified ISE staff to undertake the appropriate Information Sharing and MARAM on-line 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 any requests from ISE's are responded to in a timely manner and provide relevant information if the threshold test of the 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 or those children.	**R**	**R**	**R**		
Maintaining record keeping processes that are accurate and complete as set by *Child Wellbeing and Safety (Information Sharing) Regulations* concerning both written and verbal 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 any person is incorrect, and is corrected in a timely manner	**R**	**R**	**R**		
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 families and children	**R**	**R**	**R**		
Seeking and taking into account the views 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**		
BOLD tick **R** indicates legislation requirement					

PROCEDURES

SHARING INFORMATION AND RECORD KEEPING UNDER THE CHILD 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)*

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.

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

- *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
- *Ministerial Guidelines for the Family Violence Information Sharing Scheme:* www.vic.gov.au/family-violence-information-sharing-scheme
- *Guidelines to the Information Privacy Principles:* www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
- *Office of the Health Complaints Commissioner:* www.hcc.vic.gov.au/
- *Australia Not-for-profit Law Guide (2025), Privacy Guide: A guide to compliance with privacy laws in Australia:* Privacy-Guide.pdf
- 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 Victorian Information Commissioner:* https://ovic.vic.gov.au
- *Information sharing and Child Link: www.vic.gov.au/child-information-sharing-scheme-ministerial-guidelines*
- *Information sharing guides, templates and tools:* www.education.vic.gov.au
- *Information Sharing and Family Violence Reforms Toolkit:* www.vic.gov.au/guides-templates-tools-for-information-sharing
- *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 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
- *Family Violence Multi-Agency Risk Assessment and Management Framework:* www.vic.gov.au/family-violence-multi-agency-risk-assessment-and-management
- *Information Sharing and MARAM Online Learning System:* ww.training.infosharing.vic.gov.au/login/index.php

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

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*
- *Attachment 8: Data Breach Procedure & Response Plan*

ATTACHMENT 1. RECORD KEEPING AND PRIVACY LAWS

Early childhood services must ensure that their processes for the collection, storage, use, disclosure and disposal 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 the Nominated Supervisor/educator, to be recorded in an attendance record kept at the service. Contact details may be kept in a sealed envelope at the back of the attendance record or separate folder for evacuation/emergency purposes.
- **Medication records and incident, injury, trauma and illness records:** *Regulations 87 and 92* of the *Education and Care Services National Regulations 2011* require the Approved Provider of a service to maintain incident, injury, trauma and illness records, and medication records which contain personal and health information about the child.
- **Handling and storage of information:** Limited space can often be an issue in early childhood service environments, and both authorised employees and the Approved Provider need access to secure storage for personal and health information. Documents might be required to be stored off the service premises. Wherever confidential information is stored, it is important that it is not accessible to unauthorised staff or other persons. When confidential information is required to be taken off-site (e.g. on excursions, a list of children with medical conditions and contact numbers will be required), consideration must be given to how this is transported and stored securely.
- **Electronic records:** It is important that electronic records containing personal, sensitive or health information are stored in password protect folders or software platforms and can only be accessed by authorised personnel. Services need to incorporate risk management measures to ensure that passwords are recorded and stored in a secure folder at the service, and to limit access to the information only to other authorised persons. *(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:** A service should only collect the information it needs and for which it has a specific purpose. Services should not collect information that has no immediate use, even though it may be useful in the future.

Record Keeping Timeframes

An approved provider must keep the documents set out in the table below at the service premises if they relate to:

- the operation of the service in the previous 12 months
- any staff member employed or engaged by the service in the previous 12 months
- any child educated and cared for at those premises in the previous 12 months.

The documents must be kept in a secure place and in a manner that is readily accessible by an authorised officer.

The following table describes what records and documents must be kept and for how long. Reasonable steps must be taken to make sure the documents are accurate.

Type of Record	Responsibility	Timeframe
Evidence of all current insurance policies, including public liability **Note:** Does not apply if the insurance is provided by a state or territory government	Approved provider	Ongoing Available for inspection at service premises
Quality improvement plan	Approved provider	Ongoing, to be revised annually
Child assessments or evaluations for delivery of the educational program	Approved provider	Until the end of 3 years after the child's last attendance
Incident, injury, trauma and illness record	Approved provider	Until the child is 25 years old
Records identified as relevant to child safety and wellbeing (including child sexual abuse)	Approved provider	For at least 45 years from the date the record was created
Medication record	Approved provider	Until the end of 3 years after the child's last attendance
Child attendance record	Approved provider	Until the end of 3 years after the last date on which the child was educated and cared for by the service
Child enrolment record	Approved provider	Until the end of 3 years after the child's last attendance
Death of a child while being educated and cared for by the service	Approved provider	Until the end of 7 years after the death
Record of service's compliance history	Approved provider	Until the end of 3 years after the approved provider operated the service

Type of Record	Responsibility	Timeframe
For centre-based services, regular transportation of children records	Approved provider Nominated supervisor	Until the end of 3 years after the last date on which the child was educated and cared for by the service
Staff record	Approved provider	Until the end of 3 years after the staff member works for the service
Record of replacement of educator	Approved provider	Until the end of 3 years after the staff member works for the service
Record of replacement of early childhood teacher or suitably qualified person	Approved provider	Until the end of 3 years after the staff member works for the service
Record of access to early childhood teachers or suitably qualified person	Approved provider	Until the end of 3 years after the staff member works for the service
Record of educators working directly with children	Approved provider	Until the end of 3 years after the staff member works for the service
Record of volunteers and students, full name, address and date of birth details, days and hours in attendance, and working with children / vulnerable people check or teacher registration details	Approved provider	Until the end of 3 years after the volunteer or student attended the service
Record of responsible person in day- to-day charge including nominated supervisors placed in day-to-day charge	Approved provider	Until the end of 3 years after the staff member works for the service

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 in any financial year since 2002
- 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, as well as some private or community sector organisations, where those organisations are carrying 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 services are provided by the CSP 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 of certain health information. Early Childhood Education and Care services collect, hold and use health information, therefore are required to follow the HPP under the *Health Records Act, 2001*.

Principles in Action

Organisations need to make sure 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 is able to operate as intended.

The table below is a reference tool that identities 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	St Francis of Assisi OSHC has an up to date *Privacy and Confidentiality policy* that clearly 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 parent/guardian will have the option of not identifying themselves when entering into transactions with [Service Name]. This may include surveys, suggestion boxes, QIP 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	[Service Name] 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/guardians either in relation to themselves or a child enrolled at the service, will generally be collected via forms filled out by parents/guardians. This can include but not limited to Enrolment Records, Enrolment Application Forms, Medical Management Plans, Risk Minimisation Plans, Communication Plans, Attendance Records, Staff Records, Direct Debit Application Forms, Visitors Logbook, etc.... Other information may be collected from job applications, face-to-face interviews and telephone calls. Individuals from whom personal information is collected will be provided with a copy of the service's *Privacy Statement* *(refer to Attachment 4).* When [Service Name] receives personal information *(refer to Definitions)* from a source other than directly from the individual or the parents/guardians of the child concerned, the person receiving the information will notify the individual or the parents/guardians of the child to whom the information relates to. [Service Name] will advise that individual of their right to share or not share this information with the source. Sensitive information *(refer to Definitions)* will be collected only for the purpose of enabling 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 promotion of the wellbeing or safety of a child. 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.
APP 5 – Notification of the collection of personal information and APP 6 – Use or disclosure of personal information	IPP 2: Use and disclosure	Principle 2 Use and Disclose	Upon enrolment, commencement of employment, or any other time personal, sensitive or health information is collected, [Service Name] will take reasonable steps to ensure individuals or parent/guardian understand why this information is being collected, used, disclosed and stored. Individuals or parent/guardian will be informed of the following: • St Francis of Assisi OSHC contact details • the facts and circumstances of why personal, sensitive and health information is being collected • what information is required by authorised law • the purposes of collection • the consequences if personal information is not collected • St Francis of Assisi OSHC usual disclosures of personal information; if applicable • information about the St Francis of Assisi OSHC Privacy and Confidentiality Policy The following table identifies the personal, sensitive and health information that will be collected by St Francis of Assisi OSHC, the primary purpose for its collection and some examples of how this information will be used.

			Personal, sensitive and health information collected in relation to:	Primary purpose of collection:	Examples of how the service will use personal and health, (including sensitive) information include:
			Children and parents/guardians	• To enable the service to provide for the education and care of the child attending the service • To promote the service *(refer to Attachments 5 and 6)*	• Day-to-day administration and delivery of service • Provision of a place for their child in the service • Duty rosters • Looking after children's educational, care and safety needs • For correspondence with parents/guardians relating to their child's attendance • To satisfy the service's legal obligations and to allow it to discharge its duty of care • Visual displays in the service • Newsletters • Promoting the service through external media, including the service's website
			The Approved Provider if an individual, or members of the Committee of Management/Board if the Approved Provider is an organisation	• 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) to engage the applicant, employees, contractor, volunteers or students, as the case may be • To administer the employment, contract or placement	• Administering the individual's employment, contract or placement, as the case may be • Ensuring the health and safety of the individual • Insurance

			• Promoting the service through external media, including the service's website The service may disclose some 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 parent/guardian 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 this sensitive information is allowed by law.
APP 7 – Direct marketing	N/A	N/A	A service must not use or disclose personal information it holds for the purpose of direct marketing. Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.
APP 8 – Cross-broader disclosure of personal information	IPP 9: Transborder data flows	Principle 9 Transborder Data Flows	St Francis of Assisi OSHC will only transfer personal of health information outside Victoria in certain circumstances, for example, if the individual consents, or if the recipient of the personal information is subject to a law or binding scheme.
APP 9 – Adoption, use or disclosure of government related identifiers	IPP 7: Unique identifiers	Principle 7 Identifiers	St Francis of Assisi OSHC will not adopt, use or disclose a government related identifier unless an exception applies. 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 parent/guardian *(refer to Fees Policy)* • tax file number for all employees, to assist with the deduction and forwarding of tax to the Australian Tax Office – failure to provide this would result in maximum tax being deducted • Medicare number: for medical emergencies

			• For childcare services only: Customer Reference Number (CRN) for children attending childcare services to enable the family to access the Commonwealth Government's Child Care Subsidy (CCS) – failure to provide this would result in parents/guardians not obtaining the benefit.
APP 10 – Quality of personal information	IPP 3 - Data quality	Principle 3 Data quality	St Francis of Assisi OSHC will take reasonable steps to ensure that the personal and health information it collects is accurate, up-to-date and complete, as outlined in this Privacy and Confidentiality policy. St Francis of Assisi OSHC will ensure any updated or new personal and/or health information is promptly added to relevant existing records and will send timely reminders to individuals or parent/guardian to update their personal and/or health information to ensure records are up to date at all times. This can include but not limited to emergency contact details, authorised nominees, medical management plans, banking details, working with children checks, VIT registration etc…
APP 11 – Security of personal information	IPP 4 - Data security	Principle 4 Data Security and Data Retention	St Francis of Assisi OSHC 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)*. St Francis of Assisi OSHC will also take reasonable steps to destroy personal and health information and ensure it is de-identified if it no longer needs the information for any purpose as described in *Regulations 177, 183, 184.* In disposing of personal, sensitive and/or health information, those with authorised access to the information will ensure that it is either shredded or destroyed in such a way that the information is no longer accessible. St Francis of Assisi OSHC 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 in order to fulfil their responsibilities and duties • information will not be left in areas that allow unauthorised access to that information • all materials will be physically stored in a secure cabinet or area • computerised records containing personal or health information will be stored safely and secured with a password for access • there is security in transmission of the information via email, telephone, mobile phone/text messages, as detailed below: ○ emails will only be sent to a person authorised to receive the information ○ faxes will only be sent to a secure fax, which does not allow unauthorised access ○ telephone – limited and necessary personal information will be provided over the telephone to persons authorised to receive that information • transfer of information interstate and overseas will only occur with the permission of the person concerned or their parents/guardians.
APP 12 – Access to personal information and APP 13 –	IPP 6 - Access and correction	Principle 6 Access and Correction	Individuals or parent/guardian have the right to seek access to their own personal information and to make corrections to it if necessary. Upon request [Service Name] will give an individual or parent/guardian access to

Correction of personal information			their personal or health information it holds are part of service operations in a timely manner. [Service Name] must be satisfied through identification verification, that a request for personal or health information is granted. Process for considering access requests A person may seek access, to view or update their personal or health information: • if it relates to their child, by contacting the Nominated Supervisor • for all other requests, by contacting the Approved Provider/secretary. • Personal information may be accessed in the following way: • view and inspect the information • take notes • obtain a copy (scanned or photographed). Individuals requiring access to, or updating of, personal information should nominate the type of access required and specify, if possible, what information is required. The Approved Provider will endeavour to respond to this request within 45 days of receiving the request. The Approved Provider and employees will provide access in line with the privacy legislation. If the requested information cannot be provided, the reasons for denying access will be given in writing to the person requesting the information. In accordance with the legislation, the service reserves the right to charge for information provided in order to cover the costs involved in providing that information. The privacy legislation also provides an individual about whom information is held by the service, the right to request the correction of information that is held. The service will respond to the request within 45 days of receiving the request for correction. If the individual is able to establish to the service's satisfaction that the information held is incorrect, the service will endeavour to correct the information. There are some exceptions set out in the *Privacy and Data Protection Act 2014,* where access may be denied in part or in total. Examples of some exemptions are where: • 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 the detection, investigation or remedying of serious improper conduct and providing access would prejudice that.
N/A	N/A	Principle 10 Transfer or closure of the practice of a	N/A

		health service provider	
N/A	N/A	Principle 11 Making information available to another health service provider	N/A

ATTACHMENT 3. LETTER OF ACKNOWLEDGEMENT AND UNDERSTANDING FOR EMPLOYEES

[Place on service letterhead]

Dear[Insert Name],

Re*: Privacy and Confidentiality Policy*

Please find attached [Service Name] *Privacy and Confidentiality Policy*, which 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 requirements of the privacy legislation by ensuring they understand and implement [Service Name] *Privacy and Confidentiality Policy*. Employees need to ensure they are aware of their responsibilities in relation to the collection, storage, use, disclosure, disposal of personal and health information and the requirements for the handling of personal and health information, as set out in this policy. Therefore, all employees are required to read this policy and complete the attached acknowledgement form.

Please return the completed form below by [Date].

Yours sincerely,

[insert staff member name]

[insert staff member role]

(on behalf of the Approved Provider)

Please note: this form will be kept with your individual staff record.

[Service Name]

Acknowledgement of reading the *Privacy and Confidentiality Policy*

I, _____ , have received and read the service's *Privacy and Confidentiality Policy* and understand my responsibilities in relation to the collection, storage, use, disclosure, 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

[Place on service letterhead]

We believe your privacy is important.

[Service Name] has developed a *Privacy and Confidentiality Policy* that illustrates how we collect, use, disclose, manage and transfer personal information, including health information. This policy is available on request.

To ensure ongoing funding and licensing, our service is required to comply with the requirements of privacy legislation in relation to the collection and use of 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 for which we generally collect personal information are given in the table below.

Personal information and health information collected in relation to:	**Primary purpose for which information will be used:**
Children and parent/guardian	• To enable us to provide for the education and care of the child attending the service • To manage and administer the service as required
The Approved Provider if an individual, or members of the Committee of Management/Board if the Approved Provider is an organisation	• 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 the individual's 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/guardian 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 required 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 Approved Provider/Nominated Supervisor.

ATTACHMENT 5. PERMISSION FOR PHOTOGRAPHS AND VIDEOS

PERMISSION FOR PHOTOGRAPHS AND VIDEOS IS GRANTED AS A SUPPLEMENTARY QUESTION ON ENROLMENT/REGISTRATION

ATTACHMENT 6. SPECIAL PERMISSION NOTICE FOR PUBLICATIONS/MEDIA

[Place on service letterhead]

Use of photographs, digital recordings, film or video footage of children in media, newspapers and publications, including any service publication or media outlet

[Date]

Dear [insert name of parent/guardian],

The purpose of this letter is to obtain permission for your child to be photographed or filmed by [insert name of the organisation/individual taking the photograph or filming the child]and for your child's photograph, digital recording, film, or video footage to appear in[insert name of the newspaper, publication (including the service's publication) or media outlet where it will be displayed].

I, _____ , consent/do not consent to my child

_____ (name of child) being photographed or filmed by [insert name of the organisation/individual taking the photograph or filming the child]and for my child's photograph, digital recording, film, or video footage to appear in the following publication and/or media outlet [insert name of the newspaper,publication (including the service's publication) or media outlet where it will be displayed]

_____ _____

Signature (parent/guardian) Date

ATTACHMENT 7. SHARING INFORMATION UNDER CISS AND FVISS

This attachment has been developed based on the Information Sharing and Family Violence Reforms Contextualised Guidance: For centre-based education and care services; government, Catholic and independent schools; system and statutory bodies; and education health, wellbeing and inclusion workforces, September 2020.

Applying the threshold test under CISS

Before sharing information with other Information Sharing Entities (ISE)'s the threshold test requirements must be meet.

The requirements for sharing are different depending on the purpose of the sharing, if sharing for both purposes (Child Wellbeing or Safety and/or Family Violence), you must meet the requirements of each of the schemes.

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 for the purpose of promoting 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 to carry 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 a confidential police source • contravene a court order • be contrary to the public interest • information sharing would contravene another law.

Making a request to 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.

a. The ISE list is a searchable database that can be used to identity organisation and services prescribed under the CISS and FIVSS
b. Before making a request, check to see if the organisation is a prescribed entity via the Access the ISE list
c. Refer to Information Sharing Entity List Uses Guide on how to navigate the database.
d. ISE's should respond to requests for information in a timely manner, including when they are declining to provide information in response to the request.
e. If an ISE is declining a request from another ISE, they are required to 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 decide which organisation or service to request information from, taking into account 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 are likely to 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 make a decision about whether all three parts of the threshold have been met, in order 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 (whether the disclosure 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 ISE's

ISE's will use their expertise and exercise their professional judgement to identify:

- the range of needs and risks that impact on a child's life to inform a decision as to whether the threshold is met
- what and how much information to share
- who to share with to support improved service delivery and 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 that is 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 what information is relevant, practitioners should use their professional judgement and refer to the *Family Violence Support Policy*.

Where an ISE receives a request, it **must** share that information, either verbally or in writing, provided that the information meets the requirements of the Scheme. 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:

to establish and assess risk (Family violence assessment purpose)

Information can be shared for a family violence assessment purpose. The primary focus is on establishing whether a risk of family violence is present, assessing the level of risk the alleged perpetrator or perpetrator poses to the victim survivor, and correctly identifying the parties as the perpetrator or victim survivor.

OR

to manage the risk, including through ongoing risk assessment (Family violence protection purpose)

Information can be shared for a family violence protection purpose, which means managing the risk of the perpetrator committing family violence, or the risk of the victim survivor being subjected to family violence. Managing risk involves removing, reducing or preventing the escalation of risk. As risk is dynamic and can change over time, information can be shared for the purposes of ongoing risk assessment to monitor risk and escalation, as a key component of risk management.

All ISEs will be able to share information for a family violence protection purpose. ISEs that are also prescribed as risk assessment entities (RAEs) will also be able to shared for a family violence assessment purpose

Consent is not required from any person to share information that is relevant to assessing or managing family violence risk to a child, if there is a serious risk to any person or if sharing is permitted by another law. If none of the above apply, consent is required to share the information of an adult victim survivor, including a student over 18 years of age, or a third party. You should seek and take into account the views of the child and/or family member before sharing their information, whenever safe, reasonable and appropriate to do so. Consent is never required to share information about a perpetrator, alleged perpetrator or adolescent using or at risk of using family violence.

ISEs must not share excluded information. ISEs cannot share information that would contravene another law that has not been specifically overridden by FVISS. ISEs cannot share information if the applicable consent requirements have not been met.

To learn more about how to share information under the *Family Violence Information Sharing Scheme*, visit www.vic.gov.au/family-violence-information-sharing-scheme

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/guardian, 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 the reason 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 in order 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 the reason why

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

Examples of record keeping forms can be found at: www.vic.gov.au/guides-templates-tools-for-information-sharing

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 is sharing 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 that was taken

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

ATTACHMENT 8

DATA BREACH PROCEDURE & RESPONSE PLAN

INTRODUCTION

St Francis of Assisi OSHC is committed to managing personal information in accordance with the Commonwealth Privacy Act 1988 (Cth), Australian Privacy Principles (APPs) and the service's Privacy & Confidentiality Policy.

This document is designed to define the process the service will implement in the event of a data breach or where a suspected breach of data has occurred. A data breach occurs when personal information is lost or subject to unauthorised access, modification, disclosure, misuse or interference.

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) established a Notifiable Data Breaches Scheme (NDBS) that requires educational facilities and other organisations covered by the Act to notify any individual(s) likely to be at risk of 'serious harm' from a data breach. The NDBS also requires that the Office of the Australian Information Commissioner (OAIC) also be notified as the result of such an event.

Accordingly, St Francis of Assisi OSHC needs to be prepared to act quickly in the event of a data breach (or suspected breach), and determine whether the breach is likely to result in 'serious harm' and is eligible to be reported.

Adherence to this Procedure and Response Plan, OSHC will ensure that relevant information is forwarded to the school so they can contain, assess and respond to data breaches promptly and mitigate potential harm to the person(s) affected. St Francis of Assisi OHC will, from time to time, review and update this procedure to take account of new laws and technology, changes to the service's operations and practices and to make sure it remains appropriate to the changing OSHC environment.

DEFINITIONS

Data Breach occurs where personal information is lost or subjected to unauthorised access, modification, disclosure, misuse or interference.

Eligible Data Breach occurs where a data breach is likely to result in 'serious harm' to any individual(s) to who the information relates.

Notifiable Data Breach Scheme (NDBS 2018) An amendment to the Commonwealth Privacy Act 1988 (Cth) that requires school's & other organisations to notify an Eligible Data Breach to affected individual(s) and the Office of the Australian Information Commissioner (OAIC).

Personal Information is information or opinion, whether true or not, about a person whose identity is apparent, or can reasonably be ascertained, from the information or opinion – that is recorded in any form. For example, a person's name, address, phone number and date of birth (age). De-identified information about students can also be personal information.

Sensitive information is information or opinion about a set of specific characteristics, including a person's racial or ethnic origin, political opinions or affiliations, religious beliefs or affiliations,

philosophical beliefs, sexual preferences or practices; or criminal record. It also includes health information.

Serious Harm: May include physical, psychosocial, emotional, economic, financial harm or reputation damage resulting from any Data Breach.

SCOPE

This procedure applies to all permanent, fixed term and casual employees at St Francis of Assisi OSHC. It also extends to contractors, students and volunteers (relevant Individuals) engaged to undertake work on behalf of the service/school.

RESPONSIBILITIES

Employee Responsibilities:

- Familiarise themselves with these procedures and the services's Privacy & Confidentiality Policy;
- Respect the confidentiality of personal information they obtain and the privacy of individual(s) associated with the service;
- Immediately report any Data Breach to the Co-ordinator/Leadership Team

St Francis of Assisi OSHC responsibility:

- Ensure the security and privacy of any personal information collected by the service for educational and/or support services:
- Ensure all employees and other relevant individuals are aware of the service's Privacy & Confidentiality Policy & Notifiable Data Breach Procedure;
- Act promptly to report a Data Breach (or suspected breach), by completing the Data Breach Process Form and forward to School Principal or in their absence, the School Leadership Team or Parish Priest.

St Francis of Assisi Primary School responsibility:

- Ensure the security and privacy of any personal information collected by the service for educational and/or support services:
- Ensure all employees and other relevant individuals are aware of the service's Privacy & Confidentiality Policy & Notifiable Data Breach Procedure;
- Act promptly in the event of a Data Breach (or suspected breach), and determine whether the breach is likely to result in 'serious harm' and in turn is eligible to be reported;
- Report any Eligible Data Breach to the Office of the Australian Information Commissioner (OAIC);
- Comply with legislative requirements.

- **PROCESSES WHERE A DATA BREACH OCCURS OR IS SUSPECTED**

Alert

Where a Data Breach is known to have occurred (or is suspected) the staff member(s) who identify this must bring it to the immediate attention of the Co-ordinator, or in their absence, a member of the

Leadership Team, who will then forward details to the School Principal, or in their absence, a member of the School Leadership Team or Parish Priest.

Information that must be provided (if known) at this point includes:

a) When the breach occurred (time and date);
b) Description of the breach (type of personal information involved);
c) Cause of the breach (if known) otherwise how it was discovered;
d) Which system(s) if any are affected?;
e) Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

The service maintains a Data Breach Process Form to assist in documenting the required information (Form A).

Assess & Determine the Potential Impact

The School Principal, or in their absence, a member of the School Leadership Team or Parish Priest will determine whether a Data Breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. In determining this, the Principal may seek advice from relevant Catholic Education Commission of Victoria (CECV) representative.

Criteria for determining whether a Data Breach has occurred

The School Principal, in their absence, the School Leadership Team or Parish Priest will consider and determine whether a Data Breach has occurred:

a) Is personal information involved?;
b) Is the personal information of a sensitive nature? (Refer to Definitions);
c) Has there been unauthorised access to personal information, or unauthorised disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

Criteria for determining severity

The School Principal, or in their absence, the School Leadership Team or Parish Priest will consider when determining the severity of any Data Breach:

a) The type and extent of personal information involved;
b) The number of individuals that have been affected;
c) Whether the information is protected by any security measures (password protection or encryption);
d) The person or kinds of people who now have access to the information;
e) Whether there is or could there be a real risk of 'serious harm' (physical, psychosocial, emotional, economic, financial harm or reputation) to the affected individual(s);
f) The possibility that there could be media or stakeholder attention as a result of the breach or suspect breach.

The OSHC service maintains a Data Breach Process Form to assist the Principal or in their absence, the School Leadership Team or Parish Priest in assessing & determining the severity of any Data Breach (Form A).

'

NON-ELIGIBLE'/'ELIGIBLE' DATA BREACH

Upon review of the information provided, the Co-ordinator/Leadership Team member will work collaboratively with the school to determine whether the breach is eligible for notification to the OAIC.

To ensure an appropriate response to the identified breach, the Co-ordinator/Leadership Team member will complete a Data Breach Process Form to notify the school representative who will:

- Immediately contain the breach;
- Immediately inform all members of the School Board and other key stakeholders;
- Ensure that immediate corrective action is taken if this has not already occurred. This action may include but not be limited to informing all affected individuals of the breach;
- Retrieval or recovery of the personal information;
- Ceasing authorised access to the information;
- Shutting down or isolating the affected system;
- Prepare a briefing for Staff Members and the School Board.
-

Prepare a report containing the following:

- A description of the breach or suspected breach;
- The corrective action taken;
- Responsibilities & a timeframe for achieving the actions;
- The outcome of action taken;
- Processes to be implemented to prevent reoccurrence.

In the event there are reasonable grounds to deem the Data Breach to have the potential to cause 'serious harm' and hence be 'eligible of notification' the school representative will contact the relevant Catholic Education Commission of Victoria (CECV) representative and prepare a Notifiable Data Breach Statement. (Form B).

The Notifiable Data Breach Statement must be finalised within 30 days and be submitted to the OAIC via its website. A Notifiable Data Breach Form may also be completed 'on-line' via the OAIC website. The prescribed statement will be lodged by the school representative. Once the Notifiable Data Breach Statement has been lodged, a thorough review of all aspects to:

- Determine remedial action/s required to reduce the likelihood of reoccurrence;
- Ensure all relevant policies, procedures and processes are comprehensively reviewed and amended;
- Prepare a report / briefing for Staff Members
- Prepare a communication for the Parent Community outlining the breach, it's cause and action taken to contain, inform affected individual(s) and to prevent reoccurrence.
-

FORM A

Data Breach Process Form

A Data Breach involves the loss of, unauthorized access to, or unauthorized disclosure of personal information.

This form will assist St Francis of Assisi OSHC document the process where a Data Breach has occurred or is suspected to have occurred.

Data Breach Description

The St Francis of Assisi OSHC Co-ordinator, or in their absence, a member of the Leadership Team, are required to inform the Principal of St Francis of Assisi Primary School, or in their absence, a member of the School Leadership Team or Parish Priest within 24 hours of identifying a Data Breach or suspected breach.

Data Breach Information	
Date of Breach	
Anticipated Time of Breach	
Description of Breach	Describe the type of personal information involved, eg. Contact details, date of birth. ☐ Financial Details ☐ Contact Information ☐ Health Information ☐ Other Sensitive Information ☐ Other
Cause of Breach	*If known, describe how the Data Breach was discovered*
What System(s) if Any Are Affected	
Has Action Been Taken to Correct or Remedy the Breach?	

Other Background Information	
Reporting Staff Member	
Date	

FORM B Assessment & Determination of Potential Impact

St Francis of Assisi OSHC Co-ordinator or their absence, a member of the Leadership Team will work collaboratively with the Principal, member of the St Francis of Assisi Primary School Leadership Team or Parish Priest must consider whether a Data Breach has, or is likely to have occurred and make a preliminary determination as to the severity.

Criteria for determining whether a Data Breach has occurred	
Is Personal Information involved?	☐ Yes ☐ No
Is the Personal Information of a Sensitive Nature?	*Sensitive Information: person's racial or ethnic original political opinions or affiliations, religious beliefs, philosophical beliefs, sexual preferences or practice or criminal record* ☐ Yes ☐ No
Has there been authorised access loss, disclosure of personal information where access to the information is likely to occur?	☐ Yes ☐ No
• **Criteria for determining the severity of the Data Breach**	
What type of Personal Information was involved and to what extent?	*Names, address, phone numbers, dates of birth, academic record, student reports, financial information*
Have multiple individuals been affected?	☐ Yes *If Yes, provide details* ☐ No
Is the information protected by any security measures?	☐ Yes *If Yes, provide details* ☐ No
Provide details on the person or kinds of people who now have access to the information	• • •
Determine whether there is, or could be a real risk of 'serious harm' to the affected individuals	*Serious physical, psychosocial, emotional, economic, financial harm or reputation damage*

Determine if there could be media or external stakeholder attention as a result of the breach or suspected breach	*Media, Victoria Police, DET*
Other relevant information	
Where the Data Breach has been assessed to have the potential to cause 'serious harm', the school's <u>Notifiable Data Breach Statement</u> must be completed and submitted to the OAIC within 30 days.	

FORM C

Notifiable Data Breach Statement

This statement must be submitted to the Office of the Australian Information Commissioner (OAIC) as soon as practicable after becoming aware of an "Eligible Data Breach', and no later than 30 days, in accordance with the School's Data Breach Procedure and Response Plan.

Part 1	**Refers to requirements set out in section 26WK of the Privacy Amendment (Notifiable Data Breaches) Act 2017**
Organisation Name:	
Contact Name:	
Contact Phone Number:	
Email Address:	
Description of the Notifiable Data Breach that the school has reasonable grounds to believe has happened	
Types f Personal Information involved in the Data Breach	☐ Financial Details ☐ Contact Information ☐ Health Information ☐ Other Sensitive Information ☐ Other
Actions recommended that individuals take to reduce the risk that they experience 'serious harm' as a result of this data breach	

Other affected entities	☐ Yes *If Yes, provide further details* ☐ No

Part 2	**The information that the school provides in Part Two of this form does not need to be included in the notification(s) to affected individuals. The School may request that it be held in confidence by the OAIC.**
Data Breach:	
Date Data Breach was Discovered	
Primary Cause of the Data Breach	☐ System Fault ☐ Human Error ☐ Malicious or Criminal Act ☐ Other
A description of how the Data Breach occurred	
The anticipated number of individuals whose personal information in involved in the Data Breach	

A description of any action taken to assist individuals whose personal information was involved in the Data Breach	
A description of any action taken by the school to prevent reoccurrence	
How does the School intend to notify individuals who are likely to be at risk of serious harm as a result of the data breach	
When will this occur	
List any other data protection authorities, law enforcement bodies or regulatory bodies that you have reported this data breach to	