



PRIVACY AND CONFIDENTIALITY POLICY

Quality Area 7

PURPOSE

This policy provides a clear set of guidelines:

- for the collection, storage, use, disclosure, and disposal of personal information, including photos, videos, and health information at Rowen Street Kindergarten Inc.
- 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
- on sharing and requesting information to promote child wellbeing or safety and/or manage risk of family violence

POLICY STATEMENT

Values

Rowen Street Kindergarten Inc. is committed to:

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

Scope

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

RESPONSIBILITIES	Approved provider and persons with management or control	Nominated supervisor and persons in day-to-day charge	Early childhood teacher, educators and all other staff	Parents/guardians	Contractors, volunteers and students
R indicates legislation requirement, and should not be deleted					
Ensuring all records and documents are maintained and stored in accordance with <i>Regulations 181 and 183</i> of the <i>Education and Care Services National Regulations 2011</i>	R	√	√		√
Ensuring the service complies with the requirements of the <i>Health Privacy Principles</i> as outlined in the <i>Health Records Act 2001</i> , the <i>Information Privacy Principles</i> as outlined in the privacy and data protection act 2014 (Vic) and, where applicable, the <i>Australia Privacy Principles</i> as outlined in the <i>Privacy Act 1988 (Cth)</i> and the <i>Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)</i> , by taking proactive steps to establish and maintain internal practices, procedures, and systems that ensure compliance with privacy legalisations including: <ul style="list-style-type: none"> • 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 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 • 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 electronically accessible, is up to date and available on request	R	√			
Reading and acknowledging they have read the <i>Privacy and Confidentiality Policy</i> , including the Privacy Statement	R	√	√		
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	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	R	√	√	√	√
Providing adequate and appropriate secure storage for personal, sensitive, and health information collected by the service, including electronic storage	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, 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 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	R				
Complying with the Notifiable Data Breaches Scheme which imposes an obligation to notify individual whose personal information is in a data breach that is likely to result in serious harm.	R	√			
Promoting awareness and compliance with the Child Safe Standards and disclosing information to promote the wellbeing and safety of a child or group of children	R	R	R		
Identifying which staff should be authorised point of contact in relation to the CISS and the FVISS and that the authorised point of contact undertakes appropriate training and is aware of their responsibilities under the CISS and FVISS	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 training	R	√			
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 are met	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	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	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	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		
Only sharing confidential information 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		

Working collaboratively with services that are authorised and skilled 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	R	R	R		
Ensuring that images of children are treated with the same respect as personal information, and as such are protected by privacy laws in the same way	R	R	R	R	R
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 families 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	√			√

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 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 become operational by December 2021). 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 families 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
- Standard 7.3: Administrative systems enable the effective management of a quality service
- 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

Child Information Sharing Scheme (CISS): enables Information Sharing Entities (ISE) 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. 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 Families Act 2005](#).

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.

Disclosure: 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.

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 families 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.

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 or the new Australian Privacy Principles or any relevant code of practice.

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 and family violence services

Sources and related policies

Sources

- Child Care Service Handbook Version 2, 2019: www.dese.gov.au/resources-child-care-providers/resources/child-care-provider-handbook
- Child Information Sharing Scheme Ministerial Guidelines: www.vic.gov.au/guides-templates-tools-for-information-sharing
- 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/
- ELAA Early Childhood Management Manual: www.elaa.org.au
- Office of the Health Complaints Commissioner: <https://hcc.vic.gov.au/>
- Privacy Guide, 2020: www.nfplaw.org.au/privacy
- Australia Not-for-profit Law Guide (2017), Privacy Guide: A guide to compliance with privacy laws in Australia: www.nfplaw.org.au/sites/default/files/media/Privacy_Guide_Cth.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 Family Violence Reforms Contextualised Guidance: www.education.vic.gov.au/childhood/professionals/health/childprotection/Pages/ecunderstanding.aspx
- Information Sharing and Family Violence Reforms Toolkit: www.vic.gov.au/guides-templates-tools-for-information-sharing
- Office of the Victorian Information Commissioner, Child information sharing scheme and privacy law in Victoria: <https://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/sites/default/files/2019-01/Family%20violence%20multi-agency%20risk%20assessment%20and%20management%20framework.pdf

Service 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: Letter of acknowledgment and understanding
- Attachment 3: Privacy Statement
- Attachment 4: Sharing information and record keeping under the Child Information and Family Violence Sharing Scheme

Authorisation

This policy was adopted by the Committee of Management of Rowen Street Kindergarten Inc. on 10 October 2022

Review date: October 2026

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.
- **Forms:** Enrolment forms and any other forms used to collect personal or health information should have the service's Privacy Statement attached.
- **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.

ATTACHMENT 2. LETTER OF ACKNOWLEDGEMENT AND UNDERSTANDING FOR EMPLOYEES

Dear ,

Re: *Privacy and Confidentiality Policy*

Please find attached the *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 the *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.

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 3. PRIVACY STATEMENT

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 parents/guardians	<ul style="list-style-type: none">To enable us to provide for the education and care of the child attending the serviceTo 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	<ul style="list-style-type: none">For the management of the serviceTo comply with relevant legislation requirements
Job applicants, employees, contractors, volunteers and students	<ul style="list-style-type: none">To assess and (if necessary) to engage employees, contractors, volunteers or studentsTo 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 families 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 4. SHARING INFORMATION UNDER THE CISS AND FVISS

Applying the threshold test

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

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.

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: <ul style="list-style-type: none"> • 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 6A of the Child Wellbeing and Safety Act (and is not restricted from sharing by another law), information that could: <ul style="list-style-type: none"> • 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.

Threshold requirements for the Family Violence Information Sharing Scheme:

1	<p>The purpose of sharing is to assess family violence risk OR protect victim survivors from family violence risk.</p> <p>There are two purposes for which information can be shared between ISEs:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ establishing family violence risk ○ assessing the risk to the victim survivor ○ correctly identifying the perpetrator. <p>Family violence protection purpose: once family violence risk is established, to manage the risk to the victim survivor. This includes information sharing to support ongoing risk assessment.</p>
2	<p>The applicable consent requirements are met.</p> <p>Is the consent required when a child is at risk of family violence?</p> <ul style="list-style-type: none"> • 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 views of the child and non-violent family members where it is safe, reasonable and appropriate to do so.

- Where a student is 18 years of age or older, they are an adult and so you may need their consent to share their information, or the information of third parties, unless you can legally share under existing privacy laws or when there is a child at risk.

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 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

- 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 [Information Sharing Entity List Uses Guide](#) on how to navigate the database.
- 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.
- 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 Policy](#).

Where an ISE receives a request, it **must** share that information, either verbally or in writing, provided that the information meets the requirements (the threshold) 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:

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 a family violence protection purpose. The focus at this stage is about managing the 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 that information.
- 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 completed, 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 are documented, as a result of the information sharing.
- information is used only for a purpose permitted by law.
- if 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/s are 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, in order 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.

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.

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	
<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ 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	
<ul style="list-style-type: none"> ▪ 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 	<ul style="list-style-type: none"> ▪ Maternal and Child Health ▪ Registered out of home care services ▪ DHHS 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