# PRIVACY AND CONFIDENTIALITY POLICY

**Mandatory – Quality Area 7**

## PURPOSE

This policy will provide guidelines:

- for the collection, storage, use, disclosure and disposal of personal information, including photos, videos and health information at Eureka Community Kindergarten Association Inc. (ECKA)
- 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

### 1. VALUES

Eureka Community Kindergarten Association Inc. (ECKA) 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

### 2. 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 Eureka Community Kindergarten Association Inc. (ECKA). including during offsite excursions and activities.

### 3. 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: Governance and Leadership Management
  - Standard 7.3: Administrative systems enable the effective management of a quality service
- *Privacy and Data Protection Act 2014* (Vic)
- *Privacy Act 1988* (Cth)
- *Privacy Amendment (Enhancing Privacy Protection )Act 2012* (Cth)
- *Privacy Regulations 2013 (*Cth*)*
- *Public Records Act 1973* (Vic)

## 4. DEFINITIONS

The terms defined in this section relate specifically to this policy. For commonly used terms e.g. Approved Provider, Nominated Supervisor, Regulatory Authority etc. refer to the *General Definitions* section of this manual.

**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 Families 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:** Any information or an opinion about the physical, mental or psychological health or ability (at any time) of an individual.

***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 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.

**Personal information:** Recorded information (including images) or opinion, whether true or not, about a living individual whose identity can reasonably be ascertained.

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

***Privacy Act 1988*:** Commonwealth legislation that operates alongside state or territory Acts and makes provision for the collection, holding, use, correction, disclosure or transfer of personal information. The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) introduced from 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: *Privacy principles in action*) or the new Australian Privacy Principles (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.

## 5. SOURCES AND RELATED POLICIES

**Sources**

- 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
- 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
- ELAA Early Childhood Management Manual: www.elaa.org.au
- 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
- Guidelines to the Information Privacy Principles: www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/
- 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
- Ministerial Guidelines for the Family Violence Information Sharing Scheme: www.vic.gov.au/family-violence-information-sharing-scheme
- Office of Australian Information Commissioner, Data breach preparation and response: www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response
- Office of the Health Complaints Commissioner: https://hcc.vic.gov.au
- 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
- Office of the Victorian Information Commissioner: https://ovic.vic.gov.au
- Privacy Guide, 2020: www.nfplaw.org.au/privacy

**Service policies**

- *Child Safe Environment Policy*
- *Code of Conduct Policy*
- *Complaints and Grievances Policy*
- *Delivery and Collection of Children Policy*
- *Enrolment and Orientation Policy*
- *Information Communication and Technology Policy*
- *Staffing Policy*
- *Inclusion and Equity Policy*

## PROCEDURES

**The Approved Provider and Persons with Management and Control is responsible for:**

- ensuring all records and documents are maintained and stored in accordance with Regulations 181 and 183 of the *Education and Care Services National Regulations 2011*
- 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)
  - communicating how an individual or family can complain about any breaches of the privacy legislation, and how the service will deal with these complaints
- ensuring a copy of this policy, including the *Privacy Statement*, is prominently displayed at the service and/or electronically accessible, is up to date and available on request
- the management of privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification
- protecting personal information from misuse, interference, loss and unauthorised access, modification or disclosure, as well as unauthorised access, modification or disclosure.
- identifying and responding to privacy breaches, handling access and correction requests, and receiving and responding to complaints and inquiries
- providing regular staff training and information on how the privacy legislation applies to them and the service
- appropriate supervision of staff who regularly handle personal, sensitive, and health information
- ensuring that personal, sensitive, and health information is only collected by lawful and fair means, and is accurate and complete
- providing adequate and appropriate secure storage for personal, sensitive, and health information collected by the service, including electronic storage (refer to Attachment 2)
- ensuring that records and documents are kept in accordance with Regulation 183
- notifying an individual or family if the service receives personal, sensitive and health information about them from another source as soon as practicably possible
- 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.
- ensuring that unique identifiers are not adopted, used or disclosed unless lawfully required to (refer to Attachment 2)
- ensuring reasonable steps to destroy personal and health information and ensure it is de-identified if the information is no longer required for any purpose as described in Regulations 177, 183, 184 (refer to Attachment 1)
- complying with the *Notifiable Data Breaches Scheme* (refer to *Definitions*) which imposes an obligation to notify individual whose personal information is in a data breach that is likely to result in serious harm.
- 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.
- 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

- ensuring information sharing procedures abide by the CISS 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).
- identifying which staff should be authorised point of contact in relation to the CISS and the FVISS
- ensuring the allocated point of contact undertakes appropriate training and is aware of their responsibilities under the CISS and FVISS
- communicating to staff about their obligations under the Information Sharing Schemes (refer to *Definitions*), and ensure they have read this policy
- providing opportunities for identified ISE staff to undertake the appropriate training
- 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
- 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
- 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
- ensuring confidential information (refer to *Definitions*) 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.
- developing 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)
- 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
- 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
- working collaboratively in a manner that respects the functions and expertise of each information sharing entity
- 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.
- 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
- ensuring all employees, students and volunteers are provided with a copy of this policy, including the Privacy Statement of the service (refer to Attachment 4)
- 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
- when engaging with a professional photographer, a confidentiality clause relating to appropriate information handling is included in the agreement or contract between the photographer and the service.

**The Nominated Supervisor Persons in Day to Day Charge is responsible for:**

- assisting the Approved Provider to implement this policy
- reading and acknowledging they have read the *Privacy and Confidentiality Policy* (refer to Attachment 3)
- ensuring all records and documents are maintained and stored in accordance with Regulations 181 and 183 of the *Education and Care Services National Regulations 2011*
- protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure, as well as unauthorised access, modification or disclosure.
- ensuring that personal, sensitive and health information is only collected by lawful and fair mean, is accurate and complete

- 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
- ensuring that records and documents are kept in accordance with Regulation 183
- ensuring reasonable steps to destroy personal and health information and ensure it is de-identified if the information is no longer required for any purpose as described in Regulations 177, 183, 184 (refer to Attachment 2)
- 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)
- providing notice to children and parents/guardians when photos/video recordings are going to be taken at the service
- ensuring educators and all staff are provided a copy of this policy and that they complete the *Letter of acknowledgement and understanding* (Attachment 3)
- 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*)
- ensuring that before disclosing information under the CISS or FVISS (refer to *Definitions*), confirm that the receiving organisation or service is also an information sharing entity (refer to Attachment 7)
- ensuring any requests from an ISE's are responded to in a timely manner and provide relevant information if the threshold test of the CISS or FVISS are met (refer to Attachment 7)
- engaging with services that are authorised and skilled (including those located within The Orange Door) to determine appropriate actions and promote collaborative practice around families and children.
- 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
- working collaboratively in a manner that respects the functions and expertise of each information sharing entity
- 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*)
- being 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 when sharing information under the CISS and FVISS (refer to *Definitions*)
- promoting a child's cultural safety and recognising 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*)
- maintaining record keeping processes that are accurate and complete as set by *Child Wellbeing and Safety (Information Sharing) Regulations* in relation to both written and verbal sharing of information (refer to Attachment 7)
- 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.
- obtaining informed and voluntary consent of the parents/guardians of children who will be photographed or videoed.

**Early childhood teacher, educators and all other staff are responsible for:**

- reading and acknowledging they have read the *Privacy and Confidentiality Policy* (refer to Attachment 3)
- recording information on children according to the guidelines set out in this policy
- ensuring that personal, sensitive and health information is only collected by lawful and fair mean, is accurate and complete
- ensuring 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

- ensuring when sharing information 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*)
- engaging in training about information sharing schemes and the MARAM framework
- being aware of who the point of contact at the service under the CISS and FIVSS (refer to *Definitions*), and supporting them (if applicable) to complete the threshold test (refer to Attachment 7)
- ensuring when sharing information to promote children's wellbeing and safety, taking into consideration the child's best interests; promote collaborative practice; and give precedence to the wellbeing and safety of a child or group of children over the right to privacy
- 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*)
- being 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 when sharing information under the CISS and FVISS (refer to *Definitions*)
- working collaboratively in a manner that respects the functions and expertise of each information sharing entity
- 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*)
- 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
- respecting parents' choices about their child being photographed or videoed, and children's choices about being photographed or videoed.

**Parents/guardians are responsible for:**

- providing accurate information when requested
- maintaining the privacy of any personal or health information provided to them about other individuals, such as contact details
- completing all permission forms and returning them to the service in a timely manner
- being sensitive and respectful to other parent/guardians who do not want their child to be photographed or videoed
- being sensitive and respectful of the privacy of other children and families in photographs/videos when using and disposing of these photographs/videos.
- being aware of CISS and FVISS guidelines (refer to *Definitions*).

**Volunteers and students, while at the service, are responsible for following this policy and its procedures.**

## EVALUATION

In order to assess whether the values and purposes of the policy have been achieved, the Approved Provider of Eureka Community Kindergarten Association Inc. (ECKA) 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.

## 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: Responding to a Privacy Breach

## AUTHORISATION

This policy was adopted by the Approved Provider of Eureka Community Kindergarten Association Inc. (ECKA) on 1/08/2012.

**Operational Procedures may be modified as per the delegations policy to meet ECKA's needs.**

Reviewed 5/12/2016, 01/10/2019, 19/04/2021

## REVIEW DATE: 05/12/2022

## 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 Communication Technology Policy).
- **Forms:** Enrolment forms and any other forms used to collect personal or health information should have the service's Privacy Statement (refer to Attachment 4) 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.
- **Retention of records:**
  - records relating to an incident, illness, injury or trauma suffered by a child while at the service, until the child is aged 25 years
  - records relating to an incident, illness, injury or trauma suffered by a child that may have occurred following an incident while at the service, until the child is aged 25 years
  - records relating to the death of a child while at the service, until the end of 7 years after the death
  - and other records relating to a child enrolled at the service, until the end of 3 years after the last day on which the child attended the service
  - records relating to the approved provider, until the end of 3 years after the last date on which the approved provider records relating to a nominated supervisor or staff member of an education and care service, until the end of 3 years after the last date on which the nominated supervisor or staff member provided education at the service
  - any other records, until the end of 3 years after the date on which the record was made.

## ATTACHMENT 2
## Privacy Principles in action

**The Australian Privacy Principles**

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

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

**The Information Privacy Principles**

The IPPs are relevant for all Victorian public sector organisations, 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 Training) 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 | IPP 5: Openness | Principle 5 Openness | [Company] 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. |

| | | | |
|---|---|---|---|
| management of personal information | | | |
| APP 2 – Anonymity and pseudonymity | IPP 8: Anonymity | Principle 8 Anonymity | Wherever it is lawful and practicable, individuals and families will have the option of not identifying themselves when entering into transactions with [Company]. 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<br>IPP 10: Sensitive information | Principle 1 Collection | [Company] 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.<br>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….<br>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).<br>When [Company] 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. [Company] will advise that individual of their right to share or not share this information with the source.<br>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.<br>**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.<br>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.<br>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 disclosur | 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, [Company] will take reasonable steps to ensure individuals or families understand why this information is being collected, used, disclosed and stored. Individuals or families will be informed of the following:<br>• [Company] contact details<br>• the facts and circumstances of why personal, sensitive and health information is being collected<br>• what information is required by authorised law |

e of personal informati on

The following table identifies the personal, sensitive and health informatio [Company], the primary purpose for its collection and some examples of h used.

| **Personal, sensitive and health information collected in relation to:** | **Primary purpose of collection:** | **Examples o use persona sensitive) in** |
|---|---|---|
| Children and parents/guardians | • To enable the service to provide for the education and care of the child attending the service<br>• To promote the service (refer to Attachments 5 and 6) | • Day-to-da delivery of<br>• Provision the service<br>• Duty roste<br>• Looking at care and s<br>• For corres parents/gu child's atte<br>• To satisfy obligations discharge<br>• Visual disp<br>• Newslette<br>• Promoting external m service's v |
| 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 comm between, t other Com employees associatio<br>• To satisfy 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<br>• To administer the employment, contract or placement | • Administe employme as the cas<br>• Ensuring t the individ<br>• Insurance<br>• Promoting external m service's v |

- the purposes of collection
- the consequences if personal information is not collected
- [Service Name] usual disclosures of personal information; if applicable
- information about the [Service Name] Privacy and Confidentiality Policy

The service may disclose some personal and/or health information held

| | | | |
|---|---|---|---|
| | | | about an individual to:<br>• government departments or agencies, as part of its legal and funding obligations<br>• local government authorities, in relation to enrolment details for planning purposes<br>• organisations providing services related to staff entitlements and employment<br>• insurance providers, in relation to specific claims or for obtaining cover<br>• law enforcement agencies<br>• health organisations and/or families in circumstances where the person requires urgent medical assistance and is incapable of giving permission<br>• anyone to whom the individual authorises the service to disclose information.<br>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.<br>Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. |

| Australian Privacy Principles | Information Privacy Principles | Health Privacy Principles | Principles in action |
|---|---|---|---|
| APP 8 – Cross-broader disclosure of personal information | IPP 9: Transborder data flows | Principle 9 Transborder Data Flows | [Company] 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 | [Company] will not adopt, use or disclose a government related identifier unless an exception applies.<br>[Company] will collect information on the following identifiers (refer to *Definitions)* including but not limited to:<br>• information required to access the *Kindergarten Fee Subsidy* for eligible families (refer to Fees Policy)<br>• 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<br>• Medicare number: for medical emergencies<br>• For child care 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 | [Company] 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. [Company] 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 families 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 | [Company] 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). [Company] 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.<br><br>[Company] will ensure that, in relation to personal, sensitive and health information:<br>• 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<br>• information will not be left in areas that allow unauthorised access to that information<br>• all materials will be physically stored in a secure cabinet or area<br>• electronic 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:<br>– emails will only be sent to a person authorised to receive the information<br>– faxes will only be sent to a secure fax, which does not allow unauthorised access<br>– telephone – limited and necessary personal information will be provided over the telephone to persons authorised to receive that information<br>– 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 – Correction | IPP 6 - Access and correction | Principle 6 Access and Correction | Individuals or families have the right to seek access to their own personal information and to make corrections to it if necessary. Upon request [Company] will give an individual or families access to their personal or health information it holds are part of service operations in a timely manner. [Company] must be satisfied through identification verification, that a request for |

| | | | |
|---|---|---|---|
| of personal information | | | personal or health information is granted.<br>**Process for considering access requests**<br>A person may seek access, to view or update their personal or health information:<br>• if it relates to their child, by contacting the nominated supervisor<br>• for all other requests, by contacting the approved provider/secretary.<br>Personal information may be accessed in the following way:<br>• view and inspect the information<br>• take notes<br>• obtain a copy (scanned or photographed).<br>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.<br>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.<br>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.<br>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. [Company] 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.<br>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:<br>• the request is frivolous or vexatious<br>• providing access would have an unreasonable impact on the privacy of other individuals<br>• providing access would pose a serious threat to the life or health of any person<br>• 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 health service provider | N/A |
| N/A | N/A | Principle 11 Making | N/A |

| | | | |
|---|---|---|---|
| | | information available to another health service provider | |

## ATTACHMENT 3
## Letter of acknowledgement and understanding

[Place on service letterhead]

Dear [Insert Name],
Re*: Privacy and Confidentiality Policy*
Please find attached the [Service Name] *Privacy and Confidentiality Policy*, which outlines how [Company] 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 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 [Service Name] *Privacy and Confidentiality 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.*

Signature: _____

Date:

**ATTACHMENT 4** [Place on service letterhead]

- **Privacy statement**

[Place on service letterhead]

We believe your privacy is important.

[Company] 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 and sensitive 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 | To enable us to provide for the education and care of the child attending the service<br>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<br>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<br>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 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 5

[Place on s

**Background information**

Photographs and videos are now classified as 'personal information' under the *Privacy and Data Protection Act 2014*.

- The purpose of this permission form is to:
- comply with the privacy legislation in relation to all photographs/videos taken at the service, whether by the Approved Provider, Nominated Supervisor, educators, staff, parents/guardians, volunteers or students on placement
- enable photographs/videos of children to be taken as part of the program delivered by the service, whether group photos, videos or photos at special events and excursions etc.
- notify parents/guardians as to who will be permitted to take photographs/videos, where these will be taken and how they will be used.

**Photographs/videos taken by staff**

Staff at the service may take photographs/videos of children as part of the program. These may be displayed at the service, or placed in the service's publications or promotional material to promote the service, or for any other purpose aligned to the service's business operations. Staff may use learning journals, or learning stories on private communication programs such Storypark, in which individual and group photographs or videos are included. Parents must not screenshot or share any photos or videos containing images of children (other than their own), or other persons without the consent of the parent or other persons.

During the kindergarten year the devices that photographs or videos are recorded on, including camera memory cards, computers and electronic devices will be stored securely with password access where applicable.

When the photographs/videos are no longer being used, the service will destroy them if they are no longer required, or otherwise store them securely at the service. It is important to note that while the service can nominate the use and disposal of photographs they organise, the service has no control over those photographs taken by parents/guardians of children attending the service program or activity.

**Group photographs/videos taken by parents/guardians**

Parents/guardians may take group photographs/videos of their own child/children at special service events such as birthdays, excursions and other activities. Parents must ensure that where the photographs/videos include other children at the service they are sensitive to and respectful of the privacy of those children and families in using and disposing of the photographs/videos. Parents should not include photos or videos of staff, other parents or children other than their own, on social networking websites such as Facebook, Instagram etc, without the permission of other parents and staff.

**Photographs taken by a photographer engaged by the service**

A photographer may be engaged by the service to take individual and/or group photographs of children. Information will be provided in written form to parents/guardians prior to the event and will include the date and the photographer's details.

**Photographs/videos for use in newspapers, Eureka Community Kindergarten Association Inc. (ECKA) website and other external publications**

The permission of parents/guardians of children will, on every occasion, be obtained prior to a child's photograph being taken to appear in any electronic or printed newspaper/media, external publication and websites.

**Photographs/videos taken by students on placement**

Students at the service may take photographs/videos of children as part of their placement requirements. The permission of parents/guardians of children will, on every occasion, be obtained prior to a child's photograph being taken for this purpose.

**Access to photographs/videos**

Access to any photographs or videos, like other personal information, is set out in the service's *Privacy and Confidentiality Policy*, which is displayed at the service and available on request.

**Confirmation of consent (please tick appropriate box)**

☐ I consent to all arrangements for the use of photographs and/or videos, as stated in this permission form.

☐ I do not consent to photos or videos of my child being shared with other people. This consent overrules consent given to join Storypark.

Parent's/guardian's name Child's name

_____ _____

Signature (parent/guardian) Date

**ATTACHMENT 6**
**Special permission notice for publications/media**

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** [Place on service letterhead]

**Sharing information under the 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, April 2021.

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.

| | |
|---|---|
| 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:<br>• make a decision, an assessment or a plan relating to a child or group of children<br>• initiate or conduct an investigation relating to a child or group of children<br>• provide a service relating to a child or group of children<br>• 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:<br>• endanger a person's life or result in physical injury<br>• 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<br>• be legally privileged<br>• reveal a confidential police source<br>• contravene a court order<br>• be contrary to the public interest<br>• information sharing would contravene another law. |

*Threshold requirements for the Family Violence Information Sharing Scheme:*

| | |
|---|---|
| 1 | The purpose of sharing is to assess family violence risk OR protect victim survivors from family violence risk.<br>There are two purposes for which information can be shared between ISEs:<br>• 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:<br>– establishing family violence risk<br>– assessing the risk to the victim survivor<br>– correctly identifying the perpetrator.<br>• 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. |
| 2 | The applicable consent requirements are met.<br>Is the consent required when a child is at risk of family violence?<br>• 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.<br>• Where a child 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.<br>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.<br>Excluded information is information that could:<br>• endanger a person's life or result in physical injury<br>• prejudice a police investigation or interfere with the enforcement or administration of the law; prejudice a coronial inquest; prejudice a fair trail of a person be legally privileged<br>• reveal a confidential police source<br>• contravene a court order<br>• be contrary to the public interest<br>• information sharing would contravene another law. |

*Making a request to another Information Sharing Entity*

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

- The ISE list is a searchable database that can be used to identity 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: https://iselist.www.vic.gov.au/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*s) 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.

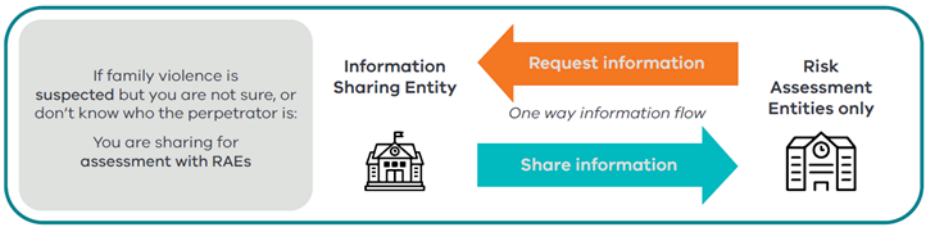


*Figure 1: Overview of activities when sharing information for risk assessment*

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

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

### *Sharing for risk management (protection):*

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

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

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

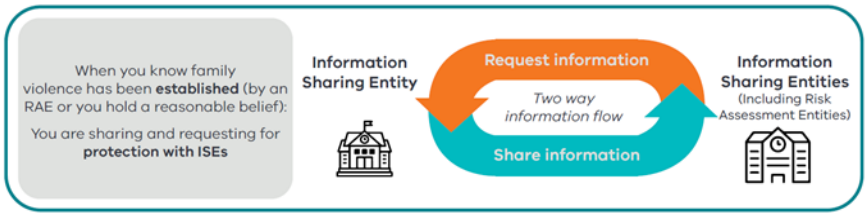


*Figure 2: Overview of activities when sharing information for risk management (protection)*

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

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

**Table 1**

| **Information Sharing Entities that are also Risk Assessment Entities** | |
|---|---|
| ▪ State-funded specialist family violence services (including refuges, Men's Behaviour Change Programs, family violence counselling and therapeutic programs)<br>▪ Risk Assessment and Management Panel (RAMP) members (including those services that would not otherwise be prescribed but only when participating in a RAMP)<br>▪ State-funded sexual assault services | ▪ Child Protection<br>▪ Child FIRST services (excluding broader family services)<br>▪ Victims Support Agency (including Victim Assistance Programs and Victims of Crime Helpline)<br>▪ Victoria Police<br>▪ The Orange Door services. |
| **Information Sharing Entities** | |
| ▪ Magistrates' Court of Victoria officials<br>▪ Children's Court of Victoria officials | ▪ Maternal and Child Health<br>▪ Registered out of home care services |

| | |
|---|---|
| ▪ Corrections Victoria and Corrections-funded services<br>▪ Adult Parole Board<br>▪ Youth Justice (including the Secretariat to the Youth Parole Board) and Youth Justice funded services<br>▪ Multi-Agency Panels to Prevent Youth Offending<br>▪ Justice Health and funded services<br>▪ State-funded sexually abusive behaviour treatment services<br>▪ State-funded perpetrator intervention trials<br>▪ Registered community-based child and family services | ▪ DHHS Housing<br>▪ State-funded homelessness accommodation or homelessness support services providing access point, outreach or accommodation services<br>▪ Designated mental health services<br>▪ State-funded alcohol and other drug services<br>▪ Tenancy Advice and Advocacy Program<br>▪ State-funded financial counselling services<br>▪ Commission for Children and Young People<br>▪ 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
## Responding to a Privacy Breach

The information Privacy Act 2000 does not require ECKA to notify individuals of a privacy breach. However, if a privacy breach creates a risk of harm or loss to the individual, those affected should be notified.

The key consideration in deciding whether to notify affected individuals is not be based on the number of affected individuals alone, rather whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed. ECKA will also take into account the ability of the individual to take specific steps to mitigate any such harm. In some exceptional cases, notification may cause more harm than it would alleviate.

**Notifying Affected Individuals**

ECKA will consider the following factors when deciding whether to notify:

- What are the legal and contractual obligations?
- What is the risk of harm, loss or damage to the individual?
- Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
- Is there a risk of humiliation or damage to the individual's reputation (e.g. when the information lost includes sensitive information or disciplinary records)?
- What is the ability of the individual to avoid or mitigate possible harm?

**When to notify:**

ECKA will notify individuals affected by the breach as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, ECKA will check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

**How to notify:**

ECKA's preferred method of notification is direct – by phone, letter, email or in person – to affected individuals. Indirect notification – website information, posted notices, media – will only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known and cannot be reasonably obtained. Using multiple methods of notification in certain cases may be appropriate. ECKA will also consider whether the method of notification might increase the risk of harm (e.g. by alerting the person who stole the laptop of the value of the information on the computer).

**Who should notify:**

ECKA will notify affected individuals, including when the breach occurs at a third-party service provider that has been contracted to collect, maintain or process the personal information. However, there may be circumstances where notification by a third party is more appropriate. For example, in the event of a breach by an organisation of credit card information, the credit card issuer may be involved in providing the notice since ECKA may not have the necessary contact information.

**Others to contact:**

ECKA will also consider whether the following authorities or organisations should also be informed of the breach, as long as such notifications are in compliance with the information privacy act:

- Police: if theft or other crime is suspected, or there is a risk to public safety;
- Health services commissioner: if any of the information is health information;
- Insurers or others: if required by contractual obligations;
- Professional or other regulatory bodies: if professional, licensing or regulatory standards require notification of these bodies;
- Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm; and
- Other internal or external parties not already notified:
  third party contractors or other parties who may be impacted; internal business units not previously advised of the privacy breach, e.g. government relations, communications and media relations, senior management, etc.

**Breaches of this Policy**

- Individuals who purposely disclose private information for any unauthosied purposes or to an unauthorized individual/s may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. The Approved Provider will not defend or support any individual who knowingly discloses private information.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.

**Prevention of Future Breaches**

Once the immediate steps are taken to mitigate the risks associated with the breach, ECKA will investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort investigating the breach should reflect the significance of the breach and whether it was a systemic breach or an isolated instance.

This plan may include the following:

- a security audit of both physical and technical security;
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (e.g. security policies, record retention and collection policies, risk management strategy etc.);
- a review of employee training practices; and
- a review of contractual obligations imposed on contracted service providers.

The resulting plan may include a requirement for a review or audit at the end of the process to ensure that the prevention plan has been fully implemented. Following any breach, it is vital that ECKA assess and evaluate how well the organisation handled the matter in line with ECKA's overall risk management strategy and make any necessary changes.

*Referenced from the Office of the Victorian Privacy Commissioner; Responding to Privacy Breaches, May 2008*