Black Rock
Pre-School

Black Rock Pre School Centre Inc.

55 Bluff Road Black Rock Vic. 3193 Phone 9598 1479
Registered Number A0002536R

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 Black Rock Pre School
- 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

Black Rock Pre School 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, Nominated Supervisor, Responsible person, educators, staff, students on placement, volunteers, parents/guardians, children and others attending the programs and activities of Black Rock Pre School.

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 *Information Privacy Act 2000* (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:

- *Education and Care Services National Law Act 2010*
- *Education and Care Services National Regulations 2011*: Regulations 181, 183
- *Freedom of Information Act 1982*
- *Health Records Act 2001* (Vic)
- *Information Privacy Act 2000* (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)
- *Public Records Act 1973* (Vic)
- *Child Wellbeing and Safety (Information Sharing) Amendment Regulations 2020*
  Family Violence Protection Amendment (Information Sharing) Act 2017

4. DEFINITIONS

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 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.

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

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

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

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

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

Risk Assessment Entity (RAE): Under FVISS, there is 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 Protection Policy*
- *Code of Conduct Policy*
- *Complaints and Grievances Policy*
- *Delivery and Collection of Children Policy*
- *Enrolment and Orientation 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 & Responsible person are 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 early childhood teachers, educators and staff are provided a copy of this policy and that they complete the Letter of acknowledgment and understanding (refer to 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.

Responsible person and other educators 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 parents/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 Black Rock Pre School 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: Additional background information
- Attachment 2: Privacy Principles in action
- Attachment 3: Privacy Statement

AUTHORISATION

This policy was adopted by the BRPS Approved Providers and Committee of Management and assessed and updated in 2020.

REVIEW DATE:

AS REQUIRED

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

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

The Australian Privacy Principles

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

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

The Information Privacy Principles

The IPPs are relevant for all Victorian public sector organisations, 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 management of personal information	IPP 5: Openness	Principle 5 Openness	[Service Name] has an up-to-date Privacy and Confidentiality policy that clearly sets out how we collect, use, disclose and store personal and health information. Stakeholders have access to this policy at any time, upon request.
APP 2 – Anonymity and pseudonymity	IPP 8: Anonymity	Principle 8 Anonymity	Wherever it is lawful and practicable, individuals and families will have the option of not identifying themselves when entering into transactions with [Service Name]. This may include surveys, suggestion boxes, QIP feedback etc.…
APP 3 Collection of solicited personal information and APP 4 – Dealing with unsolicited personal information	IPP 1: Collection IPP 10: Sensitive information	Principle 1 Collection	[Service Name] will only collect the personal, sensitive and health information needed, and for which there is a purpose that is legitimate and related to the service's functions, activities and/or obligations. Personal, sensitive and health information about children and parents/guardians either in relation to themselves or a child enrolled at the service, will generally be collected via forms filled out by parents/guardians. This can include but not limited to Enrolment Records, Enrolment Application Forms, Medical Management Plans, Risk Minimisation Plans, Communication Plans, Attendance Records, Staff Records, Direct Debit Application Forms, Visitors Logbook, etc.… Other information may be collected from job applications, face-to-face interviews and telephone calls. Individuals from whom personal information is collected will be provided with a copy of the service's *Privacy Statement* (refer to Attachment 4). When [Service Name] receives personal information (refer to *Definitions)* from a source other than directly from the individual or the parents/guardians of the child concerned, the person receiving the information will notify the individual or the parents/guardians of the child to whom the information relates to. [Service Name] will advise that individual of their right to share or not share this information with the source. Sensitive information (refer to *Definitions)* will be collected only for the purpose of enabling the service to provide for the education and care of the child attending the service. **CISS & FVISS:** Information sharing entities are not obliged to collect personal or health information about an individual directly from that person if they are collecting the information from another information sharing entity under the scheme. If an information sharing entity collects personal or health information about a person from another information sharing entity under the scheme, it will not be obliged to take reasonable steps to notify that person that their information has been collected if doing so would be contrary to the promotion of the wellbeing or

<table>
<tr><td></td><td></td><td></td><td>safety of a child.

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

• [Service Name] contact details
• the facts and circumstances of why personal, sensitive and health information is being collected
• what information is required by authorised law
• the purposes of collection
• the consequences if personal information is not collected
• [Service Name] usual disclosures of personal information; if applicable
• information about the [Service Name] Privacy and Confidentiality Policy

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

<table>
<tr><th>Personal, sensitive and health information collected in relation to:</th><th>Primary purpose of collection:</th><th>Examples of how the service will use personal and health, (including sensitive) information include:</th></tr>
<tr><td>Children and parents/guardians</td><td>• To enable the service to provide for the education and care of the child attending the service
• To promote the service (refer to Attachments 5 and 6)</td><td>• Day-to-day administration and delivery of service
• Provision of a place for their child in the service
• Duty rosters
• Looking after children’s educational, care and safety needs
• For correspondence with parents/guardians relating to their child’s attendance
• To satisfy the service’s legal obligations and to allow it to discharge its duty of care
• Visual displays in the service</td></tr>
</table>
</td></tr>
</table>

					• Newsletters • Promoting the service through external media, including the service's website
			The approved provider if an individual, or members of the Committee of Management/ Board if the approved provider is an organisation	• For the management of the service	• For communication with, and between, the Approved Provider, other Committee/Board members, employees and members of the association • To satisfy the service's legal obligations
			Job applicants, employees, contractors, volunteers and students	• To assess and (if necessary) to engage the applicant, employees, contractor, volunteers or students, as the case may be • To administer the employment, contract or placement	• Administering the individual's employment, contract or placement, as the case may be • Ensuring the health and safety of the individual • Insurance • Promoting the service through external media, including the service's website
			The service may disclose some personal and/or health information held about an individual to: • government departments or agencies, as part of its legal and funding obligations • local government authorities, in relation to enrolment details for planning purposes • organisations providing services related to staff entitlements and employment • insurance providers, in relation to specific claims or for obtaining cover • law enforcement agencies • health organisations and/or families in circumstances where the person requires urgent medical assistance and is incapable of giving permission • anyone to whom the individual authorises the service to disclose information. Sensitive information (refer to *Definitions)* will be used and disclosed only for the purpose for which it was collected, unless the individual agrees otherwise, or where the use or disclosure of this sensitive information is allowed by law.		

APP 7 – Direct marketing	N/A	N/A	A service must not use or disclose personal information it holds for the purpose of direct marketing. Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services.

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	[Service Name] 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	[Service Name] will not adopt, use or disclose a government related identifier unless an exception applies. [Service Name] will collect information on the following identifiers (refer to *Definitions)* including but not limited to: • information required to access the *Kindergarten Fee Subsidy* for eligible families (refer to Fees Policy) • tax file number for all employees, to assist with the deduction and forwarding of tax to the Australian Tax Office – failure to provide this would result in maximum tax being deducted • Medicare number: for medical emergencies • For 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	[Service Name] 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. [Service Name] 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	IPP 4 - Data security	Principle 4 Data Security and	[Service Name] 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).

information		Data Retention	[Service Name] 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. [Service Name] will ensure that, in relation to personal, sensitive and health information: • access will be limited to authorised staff, the approved provider or other individuals who require this information in order to fulfil their responsibilities and duties • information will not be left in areas that allow unauthorised access to that information • all materials will be physically stored in a secure cabinet or area • 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: – emails will only be sent to a person authorised to receive the information – faxes will only be sent to a secure fax, which does not allow unauthorised access – telephone – limited and necessary personal information will be provided over the telephone to persons authorised to receive that information – transfer of information interstate and overseas will only occur with the permission of the person concerned or their parents/guardians.
APP 12 – Access to personal information and APP 13 – Correction of personal information	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 [Service Name] will give an individual or families access to their personal or health information it holds are part of service operations in a timely manner. [Service Name] must be satisfied through identification verification, that a request for personal or health information is granted. **Process for considering access requests** A person may seek access, to view or update their personal or health information: • if it relates to their child, by contacting the nominated supervisor • for all other requests, by contacting the approved provider/secretary. Personal information may be accessed in the following way: • view and inspect the information • take notes • obtain a copy (scanned or photographed). Individuals requiring access to, or updating of, personal information should nominate the type of access required and specify, if possible, what information is required. The approved provider will endeavour to respond to this request within 45 days of receiving the request. The approved provider and employees will provide access in line with the privacy legislation. If the requested information cannot be

			provided, the reasons for denying access will be given in writing to the person requesting the information. In accordance with the legislation, the service reserves the right to charge for information provided in order to cover the costs involved in providing that information. The privacy legislation also provides an individual about whom information is held by the service, the right to request the correction of information that is held. [Service Name] will respond to the request within 45 days of receiving the request for correction. If the individual is able to establish to the service's satisfaction that the information held is incorrect, the service will endeavour to correct the information. There are some exceptions set out in the *Privacy and Data Protection Act 2014,* where access may be denied in part or in total. Examples of some exemptions are where: • the request is frivolous or vexatious • providing access would have an unreasonable impact on the privacy of other individuals • providing access would pose a serious threat to the life or health of any person • the service is involved in the detection, investigation or remedying of serious improper conduct and providing access would prejudice that.
N/A	N/A	Principle 10 Transfer or closure of the practice of a health service provider	N/A
N/A	N/A	Principle 11 Making information available to another health service provider	N/A

ATTACHMENT 3
Privacy Statement

We believe your privacy is important.

Black Rock Pre School 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*.

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 • To manage and administer the service as required
The Approved Provider - Members of the Committee of Management/Board	• For the management of the service • To comply with relevant legislation requirements
Job applicants, employees, contractors, volunteers and students	• To assess and (if necessary) to engage employees, contractors, volunteers or students • To administer the individual's employment, contracts or placement of students and volunteers

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

Disclosure of personal information, including 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.

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 Act 1981 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 or health information are able to 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 Black Rock Pre School website or on the Educa