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	HP Inc. 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 HP Inc.. 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	HP Inc. 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 HP Inc. 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. HP Inc. 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

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
			person that their information has been collected if doing so would be contrary to the promotion of the wellbeing or safety of a child. Information sharing entities will not be obliged to obtain consent from any person before collecting information under the scheme, including 'sensitive information' if they are sharing in accordance with the scheme.
APP 5 – Notification of the collection of personal information and APP 6 – Use or disclosure of personal information	IPP 2: Use and disclosure	Principle 2 Use and Disclose	Upon enrolment, commencement of employment, or any other time personal, sensitive or health information is collected, HP Inc. 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: • HP Inc. 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 • Shine Bright EYM usual disclosures of personal information; if applicable • information about the Shine Bright EYM Privacy and Confidentiality Policy

			The following table identifies the personal, sensitive and health information that will be collected by HP Inc., the primary purpose for its collection and some examples of how this information will be used. **Personal, sensitive and health information collected in relation to:** / **Primary purpose of collection:** / **Examples of how the service will use personal and health, (including sensitive) information include:** Children and parents/guardians • To enable the service to provide for the education and care of the child attending the service • To promote the service (refer to Attachments 5 and 6) • Day-to-day administration and delivery of service • Provision of a place for their child in the service • Duty rosters • Looking after children's educational, care and safety needs • For correspondence with parents/guardians relating to their child's attendance • To satisfy the service's legal obligations and to allow it to discharge its duty of care • Visual displays in the service • Newsletters • Promoting the service through external media, including the service's website The approved provider if an individual, or members of the Committee of Management/Board if the approved provider is an organisation • For the management of the service • For communication with, and between, the Approved Provider, other Committee/Board members, employees and members of the association

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
			<table><tr><td>Job applicants, employees, contractors, volunteers and students</td><td>• 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</td><td>• To satisfy the service's legal obligations • 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</td></tr></table> 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	HP Inc. 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	HP Inc. will not adopt, use or disclose a government related identifier unless an exception applies.
APP 10 – Quality of personal information	IPP 3 - Data quality	Principle 3 Data quality	HP Inc. 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. HP Inc. 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	HP Inc. 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). HP Inc. 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. HP Inc. 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

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
			– 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 HP Inc. will give an individual or families access to their personal or health information it holds are part of service operations in a timely manner. HP Inc. 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. HP Inc. 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.

Australian Privacy Principles	Information Privacy Principles	Health Privacy Principles	Principles in action
			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