ATTACHMENT 1
Additional background information

Early childhood services must ensure that their processes for the collection, storage, use, disclosure and disposal of personal and health information meet the requirements of the appropriate privacy legislation and the *Health Records Act 2001.*

The following are examples of practices 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 regarded as sensitive 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.
- *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 medical 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. It is important that confidential information is not removed from the service premises at any time, and that folders/files are not accessible to unauthorised staff or other persons attending the service.
- *Computerised records:* It is important that computerised records containing personal or health information are stored securely, and can only be accessed by authorised personnel with a password. Services need to incorporate risk management measures to ensure that passwords are recorded and stored in a secure place at the service, and to limit access to the information only to other authorised persons (refer to the *Information Technology Policy*).
- *Forms:* Enrolment forms and any other forms used to collect personal or health information should have a *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.