



7.06 Privacy and Confidentiality Policy

POLICY STATEMENT

The right to confidentiality and privacy of the child and the family is outlined in Early Childhood Code of Ethics and National Education and Care Regulations. We will respect the privacy of children and their parents and educators, while ensuring that they access high quality early years care and education in our service.

AIM

To preserve private and confidential files of the children, families, staff and visitors using the service. We aim to protect the privacy and confidentiality by ensuring continuous improvement on our current systems use, storage and disposal of records, ensuring that all records and information about individual children, families, educators and management are preserved in a secure place and are only retrieved by or released to people who need the information to fulfil their responsibilities at the service or have a legal obligation to distinguish.

STANDARDS AND PROCEDURES

Early Childhood Services are required to comply with Australian privacy law which includes the Privacy Act 1988 (the Act) which was amended in February 2017, with the changes due to take effect on February 22nd 2018.

The new law introduces a Notifiable Data Breaches (NDB) scheme that requires Early Childhood Services, Family Day Care Services and Out of School Hours Care Services to provide notice to the Office of the Australian Information Commissioner (formerly known as the Privacy Commissioner) and affected individuals of any data breaches that are “likely” to result in “serious harm.”

Businesses that suspect an eligible data breach may have occurred, must undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm to any individual affected. A failure to notify that is found to constitute a serious interference with privacy under the Privacy Act may result in a fine of up to \$360,000 for individuals or \$1.8 million for organisations.

To comply with the Privacy Act, services are required to follow the Australian Privacy Principles (APPs), which are contained in Schedule 1 of the Privacy Act 1988 (Privacy Act). In particular, the principles cover how personal information can be used and disclosed (including overseas), keeping personal information secure, and the open and transparent management of personal information including having a privacy policy.

The principles cover:

- the open and transparent management of personal information including having a privacy policy
- an individual having the option of transacting anonymously or using a pseudonym where practicable
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- how personal information can be used and disclosed (including overseas)
- maintaining the quality of personal information
- keeping personal information secure
- right for individuals to access and correct their personal information

Last published 19 September 2018

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'. Sensitive information is a type of personal information and includes information about an individual's:

- health (including predictive genetic information)
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record
- biometric information that is to be used for certain purposes
- Biometric templates.

Australian Privacy Principles (APPs)

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and Pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply

APP 3 – Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds

APP 7 – Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-order disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas

APP 9 – Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information

Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals

Management will:

- Provide Staff and Educators with relevant changes
- Make sure all relevant staff understand the requirements under Australia's privacy law
- Keep up to date with the Australian Privacy Principles (this may include delegating a staff member to oversee all privacy-related activities to ensure compliance).
- Ensure personal information is protected in accordance with our obligations under the Privacy Act 1988 and Privacy amendments (Enhancing Privacy Protection) Act 2012
- Ensure all records and documents are maintained and stored in accordance with Education and Care Service National Regulations
- Ensure the service acts in accordance with the requirements of the Privacy Principles and Privacy Act 1988 by developing, reviewing and implementing procedures and practices that identify
 - the name and contact details of the service;
 - what information the service collects and the source of information
 - why the information is collected;
 - who will have access to the information
 - Collection, storage, use, disclosure and disposal of personal information collected by the service
 - any law that requires the information to be collected;
 - adequate and appropriate storage for personal information collect by the service
 - protection of personal information from unauthorised access
- Ensure the appropriate use of images of children
- Ensure all employees, students volunteers and families are provided with a copy of this policy
- Deal with privacy complaints promptly and in a consistent manner, following the Service's Grievance Procedures. Where the aggrieved person is dissatisfied after going through the grievance process
- Ensure families only have access to the files and records of their own children
- Ensure information given to Educators will be treated with respect and in a professional manner
- Children and staff files are stored in a locked and secure cabinet
- Ensure Information relating to staff employment will remain confidential to the people directly involved with making personnel decisions.
- Information shared with us by the family will be treated as confidential unless told otherwise.

Nominated Supervisor will:

- Adhere to centre policies and procedures, supporting management
- Ensure educators, staff, volunteers and families are aware of the privacy and confidentiality policy
- Ensure the service obtains consent from parents and/or guardian of children who will be photographed or videoed by the service
- Ensure families only have access to the files and records of their own children
- Information given to Educators will be treated with respect and in a professional manner
- Ensure only necessary information regarding the children's day to day health and wellbeing is given to non-primary contact educators – for example food allergies
- Will not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand.
- Information shared with us by the family will be treated as confidential unless told otherwise.

Responsible Persons and Staff will:

- Read and adhere to the privacy and confidentiality policy at all times
- Ensure recording information and photographs of children are kept secure and may be requires at any time by the child's parents or guardian
- Ensure families only have access to the files and records of their own children
- Treat private and confidential information with respect in a professional manner
- Will not discuss individual children with people other than the family of that child, except for the purposes of curriculum planning or group management. Communication in other settings must be approved by the family beforehand.
- Information shared with us by the family will be treated as confidential unless told otherwise.
- Maintain individual and Service information and store documentation according to this policy at all times.
- Not to share information about the individual or service, management information, or other staff as per legislative authority.

Personal information our service may request regarding children:

- Parent contact details
- Emergency contact details and persons authorised to collect individual children
- Children's health requirements
- Immunisation records
- Developmental records and summaries
- External agency information
- Custodial arrangements
- Incident reports
- Medication reports
- Child care benefit and child care rebate information
- Medical records
- Permission forms

Personal information our service may request regarding staff

- Personal details
- Tax information
- Working contract
- Emergency/Medical contact details
- Immunisation details
- Working with children check
- Qualifications
- Resume
- Superannuation details
- Child Protection qualifications
- First Aid, Asthma and Anaphylaxis certificates

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS

Children (Education and Care Services) National Law NSW

- 168 - Education and care service must have policies and procedures
- 181 - Confidentiality of records kept by approved provider

SOURCE LIST

This section contains websites, industry bodies, or Legislation that have been used to assist in sourcing the information for this policy. It also acts as a guide to sourcing further reading on each relevant policy.

- [Australian Children's Education & Care Quality Authority](#)
- [Guide to the Education and Care Services National Law and the Education and Care Services National Regulations 2011](#)
- [Guide to the National Quality Standard](#)
- [ECA Code of Ethics](#)
- [Revised National Quality Standard](#)
- [Privacy Act 1988](#)
- [Australian Childcare Alliance - Changes to Australia's Privacy Law - What ECEC service need to know](#)
- [Office of the Australian Information Commission – Australian Privacy Principles guidelines](#)
- [Office of the Australian Information Commission – Australian Privacy Principles](#)

RELATED POLICIES

- 6.01 Enrolment Policy
- 7.02 Governance Policy

POLICY REVIEW

The review schedule has been developed using a risk assessment methodology with consideration given to sector, industry, and legislative changes.

Date reviewed	Policy changed		Modifications	Next Review Date
September 2018	Yes	No	Changes made to comply with changes to the Australian Privacy Act 1988, including the replacement of the National Privacy principles with the Australian Privacy Principles	October 2019