PRIVACY AND CONFIDENTIALITY POLICY

Privacy is acknowledged as a fundamental human right. Our Service has an ethical and legal responsibility to protect the privacy and confidentiality of children, individuals and families as outlined in Early Childhood Code of Ethics, Education and Care Services National Regulations and the Privacy Act 1988 (Cth).

The right to privacy of all children, their families, and educators, staff, and committee of management, of the Service will be upheld and respected, whilst ensuring that all children have access to high quality early years care and education. All staff members will maintain confidentiality of personal and sensitive information to foster positive trusting relationships with families.

PURPOSE

To ensure that the confidentiality of information and files relating to the children, families, staff, and visitors using the Service is always upheld. We aim to protect the privacy and confidentiality of all information and records about individual children, families, educators, staff, and management by ensuring continuous review and improvement on our current systems, storage, and methods of disposal of records.

We will ensure that all records and information are held in a secure place and are only retrieved by or released to people who have a legal right to access this information. We will use various methods for this to occur such as password protected ICT, lockable cabinets and necessary data blocking programs for all computers.

Our Service takes data integrity very seriously, we strive to assure all records and data is protected from unauthorised access and that it is available to authorised persons when needed.

This policy provides procedures to ensure data is stored, used and accessed in accordance with relevant policies and procedures.

SCOPE

This policy applies to children, families, educators, staff, management, approved provider, nominated supervisor and visitors of the Service.

IMPLEMENTATION

Under National Law, Section 263, Early Childhood Services are required to comply with Australian privacy law which includes the *Privacy Act 1988* (the Act) aimed at protecting the privacy of individuals. Schedule 1 of the *Privacy Act* (1988) includes 13 Australian Privacy Principles (APPs) which all services are required to apply. The APPs set out the standards, rights, and legal obligations in relation to collecting, handling, holding and accessing personal information.

The Notifiable Data Breaches (NDB) scheme 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 breach of an Australian Privacy Principle is viewed as an '*interference with the privacy of an individual*' and can lead to regulatory action and penalties.
(Source: OAIC Australian Privacy Principles)

Further information about the APPs is included in Appendix 1 of this policy.

NATIONAL QUALITY STANDARD (NQS)

QUALITY AREA 7: GOVERNANCE AND LEADERSHIP		
7.1	Governance	Governance supports the operation of a quality service
7.1.1	Service philosophy and purposes	A statement of philosophy guides all aspects of the service's operations.
7.1.2	Management Systems	Systems are in place to manage risk and enable the effective management and operation of a quality service.
7.1.3	Roles and Responsibilities	Roles and responsibilities are clearly defined and understood and support effective decision-making and operation of the service.
7.2	Leadership	Effective leadership builds and promotes a positive organisational culture and professional learning community.

EDUCATION AND CARE SERVICES NATIONAL REGULATIONS	
168	Education and care services must have policies and procedures
181	Confidentiality of records kept by approved provider
181-184	Confidentiality and storage of records

RELATED LEGISLATION

	Family Law Act 1975

RELATED POLICIES

Acceptable use of ICT resources policy Dealing with Grievances/Complaints (General) Policy Dealing with Grievances/Complaints (Staff) Enrolment & Orientation Policy Governance and Leadership Policy Section Family Communication Policy Online Privacy Policy	Interaction with Children Policy Payment of fees, Provision of fee statement policy Photograph Policy

THE APPROVED PROVIDER/ NOMINATED SUPERVISOR/ MANAGEMENT WILL:

- ensure the Service acts in accordance with the requirements of the Australian 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 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 collected by the Service.
    - protection of personal information from unauthorised access.
- ensure educators, staff, students, and volunteers have knowledge of and adhere to this policy.

- ensure families are aware of the privacy and confidentiality policy.
- provide staff and educators with relevant information regarding changes to Australian privacy law and Service policy.
- ensure all relevant staff understand the requirements under Australia's privacy law and Notifiable Data Breaches (NDB) scheme.
- maintain currency 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
- regularly back-up personal and sensitive data from computers to protect personal information collected.
- ensure all computers are password protected and install security software- antivirus protection.
- ensure families are notified of the time particular records are required to be retained as per Education and Care Services National Regulations [regulation 183 (2)]
- ensure the appropriate and permitted use of images of children, including obtaining written consent from parents and/or guardian of children who will be photographed or videoed by the service.
- 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 *Dealing with Grievances/Complaints) Policy* and procedures
- 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 and confidential 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 allergy information
- ensure individual child and staff files are stored in a locked and secure cabinet.
- ensure information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions.
- ensure any information stored by Committee of Management about Staff is returned to the Centre to be stored in that person's file in a timely manner
- the Committee of management will store information relating to meetings, staff etc in a secure place to ensure it is protected from others that are not permitted to see this

- ensure that information shared with the Service by the family will be treated as confidential unless told otherwise.
- ensure information regarding the health and wellbeing of a child or staff member is not shared with others unless consent has been provided, in writing, or provided the disclosure is required or authorised by law under relevant NSW legislation.
- complete a *Privacy Audit* every 24 months or following a breach of data to ensure the service meets lawful obligations, identifies areas for improvement and to detect potential areas of breach in privacy law.
- follow the *Data Breach Response Procedure* and complete a *Data Breach Response Template* following any breaches in data at the service.

EDUCATORS AND STAFF WILL:

- Always read and adhere to the Privacy and Confidentiality Policy.
- ensure documented information and photographs of children are kept secure but may be accessed 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.
- 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.
- ensure that information shared with the service 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 share information about the individual or service, management information, or other staff as per legislative authority.

Australian Privacy Principles- Personal Information

Moama & District Preschool Centre is committed to protecting personal information in accordance with our obligations under the *Privacy Act 1988* and *Privacy Amendments (Enhancing Privacy Protection) Act 2012.*

Personal information includes a broad range of information, or an opinion, that could identify an individual.

Sensitive information is personal information that includes information or an opinion about a range of personal information that has a higher level of privacy protection than other personal information.
(Source: OAIC-Australian Privacy Laws, Privacy Act 1988)

Personal information will be collected and held securely and confidentially about you and your child to assist our Service provide quality education and care to your child whilst promoting and maintaining a child safe environment for all stakeholders.

Personal information our Service may request regarding enrolled children:

- ☐ Child's name
- ☐ Gender
- ☐ Date of birth
- ☐ Address
- ☐ Birth Certificate
- ☐ Religion
- ☐ Language spoken at home.
- ☐ Emergency contact details and persons authorised to collect individual children.
- ☐ Children's health requirements
- ☐ Immunisation records- (Immunisation History Statement)
- ☐ Developmental records and summaries
- ☐ External agency information
- ☐ Custodial arrangements or parenting orders
- ☐ Incident reports
- ☐ Medication reports
- ☐ Medical records
- ☐ Permission forms – including permission to take and publish photographs, video, work samples.
- ☐ Doctor's contact information
- ☐ Dietary requirements

Personal information our Service may request regarding parents and caregivers.

- ☐ Parent/s full name
- ☐ Address
- ☐ Phone number (mobile & work)
- ☐ Email address
- ☐ Custody arrangements or parental agreement

Personal information our Service may request regarding staff and volunteers

- ☐ Personal details
- ☐ Tax information
- ☐ Banking details

- ☐ Working contract
- ☐ Emergency contact details
- ☐ Medical details
- ☐ Working With Children Check verification.
- ☐ Educational Qualifications
- ☐ Medical history
- ☐ Resume
- ☐ Superannuation details
- ☐ Child Protection qualifications
- ☐ First Aid, Asthma and Anaphylaxis certificates
- ☐ Professional Development certificates
- ☐ PRODA related documents such as RA number and related background checks

Method of Collection

Information is generally collected using standard forms at the time of enrolment or employment.

Additional information may be provided to the Service through email, surveys, telephone calls or other written communication.

Information may be collected online using software such as MYOB program software.

How we protect your personal information

To protect your personal and sensitive information, we maintain physical, technical, and administrative safeguards.

All hard copies of information are stored in children's individual files or staff individual files in a locked cupboard.

All computers used to store personal information are password protected. Each staff member will be provided with a unique username and password for access OWNA software. Staff will be advised not to share usernames and passwords.

Access to personal and sensitive information is restricted to key personal only.

Security software is installed on all computers and updated automatically when patches are released.

Data is regularly backed up on external drive and/or through a cloud storage solution.

Any notifiable breach to data is reported.

All staff are aware of the importance of confidentiality and maintaining the privacy and security of all information.

Procedures are in place to ensure information is communicated to intended recipients only, example invoices and payment enquiries.

Staff and Committee of Management are also aware of Acceptable use of ICT resources policy, social media Policy.

Access to personal and sensitive information

Personal and sensitive information about staff, families and children will be stored securely at all times. Families who have access to enrolment or program information online will be provided with a unique username and password. Families will be advised not to share username and passwords.

The Approved Provider will ensure that information kept in a child's record is not divulged or communicated through direct or indirect means to another person other than:

- the extent necessary for the education and care or medical treatment of the child to whom the information relates.
- a parent of the child to whom the information relates, except in the case of information kept in a staff record.
- the Regulatory Authority or an authorised officer
- as expressly authorised, permitted or required to be given by or under any Act or law
- with the written consent of the person who provided the information.

Disclosing personal and sensitive information

Our Service will only disclose personal or sensitive information to:

- a third-party provider with parent permission (for example software provider)
- Child Protection Agency- Office of the Children's Guardian and Regulatory Authority as per our *Child Protection and Providing a Child Safe Environment Policies*
- as part of the purchase of our business asset with parental permission
- authorised officers (for example public health officer)
- the regulatory authority or an authorised officer
- as expressly authorised, permitted, or required to be given by or required to be given by or under any Act or Law
- with the written consent of the person who provided the information.

Complaints and Grievances

If a parent, employee, or volunteer has a complaint or concern about our Service, or they believe there has been a data breach of the Australian Privacy Principles, they are requested to contact the Approved Provider so reasonable steps to investigate the complaint can be made and a response provided. [See: *Dealing with Grievances/Complaints Policy*]

If there are further concerns about how the matter has been handled, please contact the Office of Australian Information Commissioner on 1300 363 992 or:

https://forms.business.gov.au/smartforms/landing.htm?formCode=APC_PC

For any other general concerns, please contact the Approved Provider.

APPENDIX

The Australian Privacy Principals (APPs) outline:

- 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.

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.

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.
Source: Australian Government Office of the Australian Information Commissioner (OAIC)

https://www.oaic.gov.au/privacy/

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Privacy and Confidentiality Policy* will be updated and reviewed every three years or as a result of privacy/data breach and if critical reflection occurs in consultation with families, staff, educators and management.

SOURCE

Australian Childcare Alliance. (2019). Changes to Australia's privacy law: What ECEC services need to know: https://childcarealliance.org.au/blog/115-changes-to-australia-s-privacy-law-what-ecec-services-need-to-know
Australian Children's Education & Care Quality Authority. (2014)
Australian Government Office of the Australian Information Commission – Australian Privacy Principles: https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
Early Childhood Australia Code of Ethics. (2016).
Education and Care Services National Law Act 2010. (Amended 2018).
Education and Care Services National Regulations. (2011).
Guide to the Education and Care Services National Law and the Education and Care Services National Regulations. (2017).
Guide to the National Quality Framework. (2017). (Amended 2020).
Privacy Act 1988.
Revised National Quality Standard. (2018).
UN General Assembly (1989) United Nations Convention of the Rights of a child

REVIEW

POLICY REVIEWED BY	PRESCHOOL, FAMILIES, STAFF AND COMMITTEE		[DATE]
POLICY REVIEWED	OCT 2023	NEXT REVIEW DATE	OCT 2026
VERSION NUMBER	14092023		
MODIFICATIONS	• Policy maintenance • Policy into new template • Policy takes into consideration online data breaches •		
POLICY REVIEWED	PREVIOUS MODIFICATIONS		NEXT REVIEW DATE
5 NOV 2020	• Due for review by governance committee • Added Australian Privacy Principles and references to policies such as Online privacy policy, and Acceptable use of ICT resources.		5 NOV 2023