PRIVACY AND CONFIDENTIALITY PROCEDURE

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, National Education and Care Regulations and the Privacy Act 1988 (Cth). The right to privacy of all children, their families, and educators and staff 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.

Our Service adopts and aligns with the National Model Code and Guidelines for taking images or videos of children. (See *Safe Use of Digital Technologies and Online Environments Policy*).

Working in conjunction with the *Privacy and Confidentiality Policy*, this procedure ensures that the confidentiality of information and files relating to the children, families, staff, and visitors using the Service is upheld at all times.

Education and Care Services National Law or Regulations *(R.168, 170, 171, 177, 181, 183 and 184) NQS QA 7: Element 7.1, 7.1.1, 7.1.2, 7.1.3 and 7.2 Governance practices and procedures*
Related Policy: *Privacy and Confidentiality Policy and Safe Use of Digital Technologies and Online Environments Policy*

STEP 1: COLLECTION OF DATA		
1	East Lismore Community Preschool ABN 88736987995 is committed to protecting personal information in accordance with our obligations under the Privacy Act 1988 and Privacy Amendments (Enhancing Privacy Protection) Act 2012	
2	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*	
3	Personal information our Service may request regarding enrolled children: ☐ Child's name ☐ Gender ☐ Date of birth ☐ Birth Certificate ☐ Address	

	☐ 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 ☐ Child Care Subsidy information ☐ Medical records ☐ Authorisation forms – including authorisation to take and publish photographs, video, work samples ☐ Doctor's contact information ☐ Centrelink Customer Reference number (CRN) ☐ Dietary requirements	
4	Personal information our Service may request regarding parents and caregivers ☐ Parent/s full name ☐ Address ☐ Phone number (mobile & work) ☐ Email address ☐ Bank account or credit card detail for payments ☐ Centrelink Customer Reference number (CRN) ☐ Family court documentation- custody arrangements or parental agreement ☐ Any other information related to Family Assistance Law	
5	Personal information our Service may request regarding staff and volunteers ☐ Personal details ☐ Tax information ☐ Banking details ☐ Working contract ☐ Emergency contact details ☐ Medical details ☐ Immunisation 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 background checks	

STEP 2: METHOD OF COLLECTION OF INFORMATION		
1	Information is generally collected using standard forms at the time of enrolment, engagement or employment	
2	Additional information may be provided to the Service through email, surveys, telephone calls or other written communication	
3	Information may be collected online through the use of software OWNA	

STEP 3: STORAGE OF PERSONAL INFORMATION		
1	To protect personal and sensitive information, our Services maintains physical, technical and administrative safeguards. All personnel records, personal records related to children and families, and other records related to the Service's provision of education and care will be stored securely and only accessed by authorised personnel.	
2	All hard copies of information will be stored in children's individual files or staff individual files in a locked cupboard or filing cabinet	
3	The approved provider will determine who is authorised to access private and sensitive information	
4	All computers used to store personal information are password protected. Each staff member will be provided with a unique username and password for access to program software. Staff are not permitted to share usernames and passwords. Staff are encouraged to change passwords every 6 months.	
5	Access to personal and sensitive information is restricted to key personal only	
6	Security software is installed on all computers and updated automatically when patches are released	

7	Data is regularly backed up on external drive and/or through a cloud storage solution	
8	Any notifiable breach to data is reported	
9	All staff are bound to respect the privacy rights of children, families, other personnel of the Service	
10	All staff must sign a *Confidentiality Agreement* to maintain the privacy and security of information and agree to delete any confidential information from personal devices, surrender documentation, software and any other materials related to the Service upon ceasing employment with the Service.	
11	Procedures are in place to ensure information is communicated to intended recipients only.	
12	The approved provider will ensure all nominated supervisors, educators, staff, visitors and volunteers are aware of and strictly adhere to the National Mode Code guidelines including: • adhering to the *Safe Use of Digital Technologies and Online Environments Policy* • only service-issued/approved devices are to be used when taking images or videos of children • personal electronic devices that can take images or videos (such as tablets, phones, digital cameras, smart watches, META glasses) and personal storage and file transfer media (such as SD cards, USB drives, hard drives and cloud storage) are not in the possession of any educator, staff member, visitor or volunteer while providing education and care and working directly with children • Service-issued devices are stored securely and are not removed from Service premises (unless for operational activities such as excursions or transportation) • ensure staff or volunteers submit a written request if seeking an exemption to use or have in their possession a personal electronic device for essential purposes • strict controls are in place for the appropriate storage and retention of images and videos in accordance with our *Record Keeping and Retention Policy* • parents/guardians are required to provide written authorisation for the use, storage and destruction of digital documentation, including images and videos • personal information is de-identified or destroyed and removed from storage, in accordance with the *Record Keeping and Retention Policy* • images and videos are destroyed and removed from storage if a parent/guardian revokes their authorisation	

STEP 4: ACCESS TO PERSONAL AND SENSITIVE INFORMATION		
The approver provider will:		
1	ensure personal and sensitive information about staff, families and children will be stored securely at all times	

2	provide families with a unique username and password when they access enrolment or program information online. Families will be advised not to share username and passwords.	
3	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.	
4	determine who is authorised to take, use, store and destroy images and videos of children	
5	ensure service-issued electronic devices are secure using password protected systems	
6	provide access to private and sensitive information to authorised personnel only, ensuring unique username and passwords are used and not shared between others	

STEP 5: DISCLOSING PERSONAL AND SENSITIVE INFORMATION		
1	Our Service will only disclose personal or sensitive information to: - a third-party provider with parent permission - Child Protection Agency- Office of the Children's Guardian and Regulatory Authority as per our *Child Protection and Child Safe Environment Policies* - as part of the purchase of our business asset with parental permission *OR* - under relevant state/territory legislation to ensure the safety, health and wellbeing of a child.	

STEP 6: COMPLAINTS AND GRIEVANCES		
1	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	
2	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 Lodge a privacy complaint online	
3	For any other general concerns, parents and families are requested to contact the approved provider directly on: 0429107762	

REVIEW OF PROCEDURE			
Date procedure created	15.6.2026	To be reviewed	June 2027
Approved by	Michelle Donadel	Signature	
Location of procedure	Dropbox/policy folder/OWNA		
Procedure reviewed date	Modifications/Changes		
September 2025	Procedure updated to include additional practices in alignment with the National Model Code		

PRIVACY AND CONFIDENTIALITY RESOURCES		
NAME OF RESOURCE	RESOURCE DESCRIPTION	DESKTOP LIBRARY LOCATION
POLICY AND PROCEDURES		
Privacy and Confidentiality Policy	This policy aims 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 of our current systems, storage, and methods of disposal of records.	QA7 Policy Library
Safe Use of Digital Technologies and Online Environments Policy	The *Safe Use of Digital Technologies and Online Environments Policy* outline conditions required by the Service regarding transporting children as per National Regulations and related legislation	QA2 Policy Library
Privacy and Confidentiality Procedure	This procedure ensures that the confidentiality of information and files relating to the children, families, staff, and visitors using the Service is upheld at all times.	Resources > Procedures
Safe Use of Digital Technologies and Online Environments Procedure	This procedure provides clear guidance to ensure the safe and responsible use of digital devices and online environments by children, families, staff, educators, students and volunteers whilst at the Service.	Resources > Procedures
Privacy Law Compliance Procedure	This procedure provides detailed steps on how management can manage sensitive personal information and react to data breaches.	Resources > Procedures
Data Security Checklist	This checklist is available for new staff and educators to acknowledge their responsibility to ensure data is stored, used and accessed in accordance with relevant policies and procedures.	Resources > Checklists
Confidentiality Agreement	Employees and volunteers are required to sign a *Confidentiality Agreement* upon employment and engagement to protect sensitive information from being shared, disclosed or used improperly.	Resources > Forms

Data Breach Response Record	This record will enable management to contain, evaluate the risks and consider the breach and review and review to a data breach.	Resources > Forms
Digital Technologies and Online Environments Risk Assessment	This risk assessment action plan identifies potential hazards related to the use of digital technologies and online environments within our Service and specifies actions (control measures) to be taken to minimise or control those risks.	Resources > Forms
Privacy Audit	The *Privacy Audit* will help Services to meet their lawful obligations, identify areas for improvement and detect potential areas of breach in privacy law.	Resources > Audits
Media Authorisation Child	The *Media Authorisation - Child* form requests authorisation from families for the capture, use, storage, and sharing of their child's images and videos in accordance with the Service policies, including sharing images and videos in media such as social media or Service websites.	Resources > Forms
Media Authorisation Staff	The *Media Authorisation - Staff* form requests authorisation from staff and educators for images and videos to be included in media, including online media.	Resources > Forms