PRIVACY AND CONFIDENTIAL POLICY

Related Quality Area	QA7: Governance & Leadership
Related Policies	Enrolment & Orientation Policy Photograph Policy Social Media Policy Code of Conduct Policy Record Keeping & Retention Policy Governance Policy Grievance (Families) Policy

PURPOSE

To ensure that the confidentiality of information and files relating to the children, families, staff, and visitors using the Centre is upheld at all times. The Nightcliff Family Centre (the Centre) 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 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.

SCOPE

This policy applies to children, families, staff, management, and visitors of the Centre.

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 are included in Appendix 1 of this policy.

The Approved Provider/ Management will:

- ensure the Centre 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 Centre
  - what information the Centre 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 Centre
- any law that requires the particular information to be collected
- adequate and appropriate storage for personal information collected by the Centre
- protection of personal information from unauthorised access.

- 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
- ensure all computers are password protected and install security software- anti virus 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)] if this information is requested.
- ensure the appropriate and permitted use of images of children (refer to the Centre's Photograph Policy and Social Media Policy).
- 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 Centre's policies and procedures (refer to Grievance Policy (Staff) and Grievance Policy (Families).
- 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 individual child and staff files are stored in a secure cabinet
- ensure information relating to staff employment will remain confidential and available only to the people directly involved with making personnel decisions
- ensure that information shared with the Centre by the family will be treated as confidential unless told otherwise.

A Nominated Supervisor and/or Responsible Person will:

- adhere to Service's policies and procedures at all times
- ensure Educators, staff, volunteers, and families are aware of the *Privacy and Confidentiality Policy*.
- ensure the Centre obtains written consent from parents and/or guardian of children who will be photographed or videoed by the Centre
- ensure families only have access to the files and records of their own children
- ensure that information given to Educators will be treated with respect and in a confidential and 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 allergy information.
- 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 us by the family will be treated as confidential unless told otherwise.
- require new employees, volunteers, students and casuals to sign a Confidentiality Agreement as part of their induction and orientation process
- full time employees to sign a Confidentiality Agreement every two years

Educators and staff will:

- read and adhere to the *Privacy and Confidentiality Policy* at all times.
- 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 Centre 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.

Personal information our Service may request regarding enrolled children:

- ☐ Child's name
- ☐ Gender
- ☐ Date of birth
- ☐ 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
- ☐ Child Care Subsidy information
- ☐ Medical records
- ☐ Permission forms – including permission to take and publish photographs, video, work samples
- ☐ Doctor's contact information
- ☐ Centrelink Customer Reference number (CRN)
- ☐ Dietary requirements
- ☐ Court orders which include reference to a child at the centre (DVO, AVO etc.)
- ☐ Any criminal court proceedings in which a child of the centre is directly involved

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)
- ☐ 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
- ☐ 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

Method of Collection

Information is generally collected using standard forms at the time of enrolment.
Additional information may be provided to the Centre through email, surveys, telephone calls or other written communication.

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 in a locked cupboard.
All computers used to store personal information are password protected.
Access to personal and sensitive information is restricted to key personal only.
Security software is installed on all computers
Any notifiable breach to data is reported
All staff are aware of the importance of confidentiality and maintaining the privacy and security of your information.

Access to personal and sensitive information

Personal and sensitive information about you and your child will be stored securely at all times. 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 CCS software provider)
- Child Protection Agency- Office of the Children's Guardian and Regulatory Authority as per our *Child Protection and Child Safe Environment Policies*

BREACH OF POLICY

Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment, staff members who engage in unauthorised disclosure of confidential or sensitive personal information may face disciplinary action. Visitors or volunteers who fail to comply to this policy may face termination of their engagement.

Complaints and Grievances

If a parent, employee or volunteer has a complaint or concern about our Centre, 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.
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

APPENDIX 1

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/

REVIEW

POLICY REVIEWED	May 2022	NEXT REVIEW DATE	May 2024
MODIFICATIONS	• No modifications		

POLICY REVIEWED BY	Judy Rondon	Director	May 2024
POLICY REVIEWED	May 2024	NEXT REVIEW DATE	May 2026
MODIFICATIONS	• additional information added re: • "BREACH OF POLICY Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment, staff members who engage in unauthorised disclosure of confidential or sensitive personal information may face disciplinary action. Visitors or volunteers who fail to comply to this policy may face termination of their engagement". • "require new employees, volunteers, students and casuals to sign a Confidentiality Agreement as part of their induction and orientation process" • "full-time employees to sign a Confidentiality Agreement every two years "		