# Gumnut Kindergarten

## PRIVACY AND SECURITY POLICY

### Purpose

This policy is to address the issues of privacy and security of children, educators, volunteer workers and parents using the service along with their information. It aims to protect the privacy and confidentiality by ensuring that all records and information about individual children, families, educators, and management are kept in a secure place and are only accessed by or disclosed to those people who need the information to fulfil their responsibilities at the service or have a legal right to know according to National Regulation requirements and Privacy Act requirements.

### Strategies

**Australian Privacy Principles**

**Australian Privacy Principle 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.
**Australian Privacy Principle 2**—Anonymity and pseudonymity
Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
**Australian Privacy Principle 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.
**Australian Privacy Principle 4**—Dealing with unsolicited personal information
Outlines how APP entities must deal with unsolicited personal information.
**Australian Privacy Principle 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.
**Australian Privacy Principle 6**—Use or disclosure of personal information
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
**Australian Privacy Principle 7**—Direct marketing
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
**Australian Privacy Principle 8**—Cross-border disclosure of personal information
Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
**Australian Privacy Principle 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.
**Australian Privacy Principle 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.
**Australian Privacy Principle 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.

**Australian Privacy Principle 12**—Access to personal information

Outlines an APP entity's obligations when an individual requests 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.

**Australian Privacy Principle 13**—Correction of personal information

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

## Sensitive 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
- biometric templates (Anything that can uniquely identify a person based on physical characteristics of their body eg. Fingerprints)

## What is a 'Data Breach'?

1. Unauthorised Access to personal information by someone who is not permitted to have access.
2. Unauthorised Disclosure; unintentionally, negligently or intentionally makes personal information accessible to others outside the entity and releases that information from its effective control in a way that is not permitted by the Privacy Act.
3. Loss which refers to the accidental or inadvertent loss of personal information held by an entity, in circumstances where it is likely to result in unauthorised access or disclosure.

Notifiable Data Breaches (NDB) scheme requires all businesses regulated by the Privacy Act (including ECEC services) to provide notice to the Office of the Australian Information Commissioner and affected individuals of any data breaches (ie. data leaks) 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.

## The nature of the harm

In assessing the risk of serious harm, entities should consider the broad range of potential kinds of harms that may follow a data breach. It may be helpful for entities assessing the likelihood of harm to consider a number of scenarios that would result in serious harm and the likelihood of each. Examples may include:

- identity theft
- significant financial loss by the individual
- threats to an individual's physical safety

- loss of business or employment opportunities
- humiliation, damage to reputation or relationships
- workplace or social bullying or marginalisation

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

Families are not obliged to provide all personal information upon enrolment at the service, however, not providing this information could prohibit the service from providing you with a full range of services to your family.
Any confidential or personal data that is stored on the computers relating to staff and families will be protected with passwords that only the allocated responsible persons have access to.

Any online documentation is secured and only families with children enrolled in the service are allowed to access the information. Each family will have their own login details and these details are not allowed to be shared. Families are to sign a permission form for their child's information to be put up on the online program along with photos of their child.

## Responsibilities of the Approved Provider

- Ensure that your service, including the Nominated Supervisor and all of the staff are abiding by the guidelines set out in the *Privacy Act* 1988 (Cth), as well as all of the guidelines set out on the Office of the Australian Information Commissioner (OAIC) website.
- The childcare service should be provided with cameras, USB sticks, and computer devices for handling their work so as not to use their own devices from home, most importantly, using their own personal mobile telephones, laptops or tablets.
- Child, family, staff, volunteer, and student information will be disposed of appropriately when no longer needed, or are no longer required to be kept by law. Files that are required to remain on premises for a certain amount of time will be kept on premises but handled in a secure manner to protect any data breach.
- Parents must give permission for any photos or child information to be shared on any website or advertising material.
- Service CCTV footage should never be shared outside of the service unless authorities request it when under investigation.
- Only reasonable personal information will be collected from families which is relating directly to requirements the Approved Provider must provide.
- Documentation that is no longer required will be destroyed appropriately to prevent personal information from being access elsewhere.

## Responsibilities of the Nominated Supervisor

- Ensuring that the children's and all staff files are safely locked away.
- Only selected staff have access to the children and staff files.
- Before displaying information on any children, make sure that you have received parental permission.
- Before the service is allowed to hand out information to schools regarding the child, the school and childcare service must first get the parent's (carer's or guardian's) permission to do so before passing on any such information in respect of either a child still enrolled at the service, or who has been previously enrolled at the service. Such permission should be in writing and specify the content and nature of any such information being so provided.

## Responsibilities of the Educators

- Information about a child in the service should not be shared with any other families unless permission is given by that child's family in writing.
- A child's privacy should also be respected. Accordingly, when discussing any sensitive matter in respect of any such child, it should be done in private, and not in front of the child.
- Staff are not allowed to use their own personal technology for child use within the service and this includes laptops, tablets, mobile phones and cameras. Wherever possible this requirement should be spelt out in their individual contracts of employment, or at the very least, in a policy of the centre.
- Encourage families to only look through their own child's records (portfolios/observations).

## Responsibilities of the Families

- You are allowed to have access to your child's file at any time as long as an allocated responsible person is present and assists.
- CCTV Footage is captured throughout the service and is only available for viewing in emergency situations or for any investigatory reasons. Footage will not be shared anywhere besides authorities should it be required.

## Definitions, Terms & Abbreviations

| Term | Meaning |
|---|---|
| Breach | An act of breaking or failing to observe a law, agreement or code of conduct |
| CCTV | Closed Circuit Television |

## Related Statutory Obligations & Considerations

**Australian Children's Education and Care Quality Authority (ACECQA)**
http://www.acecqa.gov.au/
**Department of Education** - http://www.dec.nsw.gov.au/what-we-offer/regulation-and-accreditation/early-childhood-education-care
**Early Years Learning Framework (EYLF)** - http://files.acecqa.gov.au/files/National-Quality-Framework-Resources-Kit/belonging_being_and_becoming_the_early_years_learning_framework_for_australia.pdf
**Education and Care Services National Regulations 2011**
http://www.legislation.nsw.gov.au/#/view/regulation/2011/653
**National Quality Framework (NQF)** - http://acecqa.gov.au/national-quality-framework/
**Office of the Australian Information Commissioner** - https://www.oaic.gov.au/
**United Nations Convention on the rights of the child -** https://www.unicef.org.au/

## Related Telephone Numbers

- Early Childhood Directorate – 1800 619 113
- OAIC – 1300 363 992

## Amendment History

| Version | Amendment | Short Description |
|---|---|---|
| 1 | Updated | New Policy to comply with legislation. |

This policy will be updated to ensure compliance with all relevant legal requirements every year. Appropriate consultation of all stakeholders (including staff and families) will be conducted on a timely basis. In accordance with Regulation 172 of the *Education and Care Services National Regulation*, families of children enrolled will be notified at least 14 days and their input considered prior to any amendment of policies and procedures that have any impact on their children or family.

| | |
|---|---|
| Date: | 7 August 2018 |
| Version: | 1 |
| Last Amended By: | Patricia Appleby |
| Next Review: | 2019 |
| Position: | Director |