WINTON SHIRE COUNCIL
LITTLE SWAGGIES CHILD CARE CENTRE

CONFIDENTIALITY & PRIVACY POLICY & PROCEDURE

CONFIDENTIALITY & PRIVACY – POLICY & PROCEDURE

Table of Contents

POLICY STATEMENT

Winton Shire Council (WSC) Little Swaggies Child Care Centre is committed to protecting the privacy and confidentiality of individuals by ensuring that sensitive information about individual children, families, team members and management are kept in a secure place and are only accessed by, or disclosed to, those people who need the information to fulfill their responsibilities at the Centre or have a legal right to know.

This Policy embodies this commitment and applies to personal information collected by Little Swaggies Child Care Centre.

SCOPE

The following is required under the Education and Care Services National Regulations:

"Subdivision 4—Confidentiality and storage of records

- **181 – Confidentiality of records kept by approved provider**
    - Information kept in a record must not be divulged or communicated, directly or indirectly, to another person other than:
        - Where necessary for medical treatment of a child
        - To a parent of a child
        - To the regulatory authority or authorised officer
        - Expressly authorised, permitted or required under any Act or law
        - With the written consent of the person who provided the information.

We adhere to the requirements of the *Information Privacy Principles* contained within the *Privacy Act* and the Guidelines for Federal and ACT Government World Wide Websites, issued by the Office of the Australian Information Commissioner and Privacy Commissioner.

"The Privacy Act defines 'personal information' as: Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a. Whether the information or opinion is true or not; and
b. Whether the information or opinion is recorded in a material form or not.

The term 'personal information' encompasses a broad range of information. A number of different types of information are explicitly recognised as constituting personal information under the Privacy Act. For example, the following are all types of personal information:

- *'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information)*
- *'health information' (which is also 'sensitive information')*
- *'credit information'*
- *'employee record' information (subject to exemptions), and*
- *'tax file number information'.*

Common examples of personal information:

1. *Information about a person's private or family life.*
    - *A person's name, signature, home address, email address, telephone number, date of birth, medical records, bank account details and employment details will generally constitute personal information.*
2. *Information about a person's working habits and practices.*
    - *A person's employment details, such as work address and contact details, salary, job title and work practices.*
    - *Certain business information — for example, information about a loan taken out by a sole trader to purchase tools for their business, or information about utility usage — may be personal information about the sole trader.*
3. *Commentary or opinion about a person.*

- *In certain circumstances, a referee's comments about a job applicant's career, performance, attitudes and aptitude is 'personal information' as it is information about that person. The referee's comments may also be personal information about the referee given that they provide information about the referee's views on a particular subject. Likewise, a trustee's opinion about a bankrupt's affairs and conduct can be personal information about both the bankrupt and the trustee.*
- *An opinion about an individual's attributes that is based on other information about them, such as an opinion formed about an individual's gender and ethnicity, based on information such as their name or their appearance. This will be personal information about the individual even if it is not correct.*
- *Information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history."*[1]

"Why do ECEC services have to comply with privacy law?

Under Australia's privacy law, ECEC services are deemed as health service providers, which puts them in the category of an "Australian Privacy Principle (APP) Entity". Under Australian law, all APP entities are bound by the Act and must comply with it.

Your Responsibilities

In order to comply with the Privacy Act, ECEC services are required to follow the Australian Privacy Principles (APPs), which are contained in schedule 1 of the Privacy Act 1988 (Privacy Act).

The APPs outline how ECEC services (and other relevant businesses) must handle, use and manage the personal information of their clients. 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 new law introduces a Notifiable Data Breaches (NDB) scheme that requires all businesses regulated by the Privacy Act (including ECEC 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 (i.e. data leaks) that are "likely" to result in "serious harm. "[2]

"What should you do if you become aware of a serious data breach?

When a business/organisation becomes aware of reasonable grounds to believe an eligible data breach has occurred, they are obligated to promptly notify individuals at likely risk of serious harm. The Office of the Australian Information Commissioner must also be notified as soon as practicable through a statement about the eligible data breach. You can find out more about the Notifiable Data Breaches scheme, and the mandatory notification process here.

Definition Of Eligible Data Breach

An eligible data breach arises when the following three criteria are satisfied:

- *there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds*
- *this is likely to result in serious harm to one or more individuals and*
- *the entity has not been able to prevent the likely risk of serious harm with remedial action*

[1] "what is personal information" Australian Government Office of the Australian Information Commissioner (accessed on-line March 2020) https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

[2] Information factsheet provided by Australian Childcare Alliance December 2017 (accessed on-line Feb 2021) https://nsw.childcarealliance.org.au/news/295-reminder-changes-to-privacy-law-for-ecec-services

If there is a possible data breach the service must seek further information from the Office of the Australian Information Commissioner, details can be found at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches#key-points

Where notifiable data breach has been determined the service must use the Notifiable Data Breach Form located at https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

*"An entity must take all reasonable steps to complete the assessment within **30 calendar days** after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach (s 26WH(2)).*

The Commissioner expects that wherever possible entities treat 30 days as a maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

Where an entity cannot reasonably complete an assessment within 30 days, the Commissioner recommends that it should document this, so that it is able demonstrate:

- *that all reasonable steps have been taken to complete the assessment within 30 days*
- *the reasons for the delay*
- *that the assessment was reasonable and expeditious*" [3]

"Responding to Data Breaches – four key steps

- ***Step 1: Contain** the data breach to prevent any further compromise of personal information.*
- ***Step 2: Assess** the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.*
- ***Step 3: Notify** individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.*
- ***Step 4: Review** the incident and consider what actions can be taken to prevent future breaches."*[4]

"Protecting your business from a cyber-attack

- *Be sure staff only have access to what they need; don't grant universal access across a business*
- *When staff leave the business, remove all access and permissions immediately*
- *Create strong passwords*
- *Engage IT security experts to assist with your cyber security*
- *Train all staff about the risk of a cyberattack and the prevention strategies in place*
- *Regularly back up data and information"*[5]

Visit ACSC Australian Cyber Security Centre https://www.cyber.gov.au/ for more resources and guides

[3] "Identifying eligible data breaches" Office of the Australian Information Commissioner (accessed on-line Feb 2021) https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches#key-points

[4] "Assessing a suspected data breach" Office of the Australian Information Commissioner (accessed on-line Feb 2021) https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach

[5] *"Business Cyber Security Obligations"* Guild Insurance Jan 2018

PROCEDURE

Responsibilities of Leadership, Management, Nominated Supervisors and Responsible Persons:

- Positively and clearly communicate all aspects of the policy and take a zero-tolerance approach to compliance.
- Understand and comply with all aspects of this policy and related legislation and support team members to do the same.
- Lead a culture of reflection and regular review of policies, seeking feedback from educators, families, children and other community agencies and professionals as appropriate.
- Only collect information:
    - if it is required for providing education and care or for employment purposes
    - using lawful means and with the express permission of the person to whom the information directly relates to, this may include from a parent/guardian when relating to information about a child.
- Seek permission to display health information such as allergies or life-threatening medical conditions in both the enrolment form and any forms related to medical conditions. Ensure personal and confidential information is stored securely using lockable devises or passwords. Do not leave confidential or personal information in accessible areas.
- Only disclose sensitive and private information where required for the provision of education and care, for child protection or where required by law. This includes information shared with third parties such as for Child Care Subsidy or with the regulatory authority.
- Ensure families have access to information kept at the service in relation to themselves and their children except where documents are protected in a court order.
- Ensure permission is sought on Enrolment Forms for use of photographs.
- Never share or store passwords in an accessible way.
- Ensure credit card details are not stored in an accessible way. They should be encrypted, be incomplete or marked in a way that conceals to prevent unauthorised use.
- Conduct private and sensitive conversations in a private location and where possible in the absence of children.
- Dispose of personal information using a shredder or similar devise.

Adopt the following principles for handling personal information based on the Privacy Act (1988):

- Collection of information will be lawful and fair.
- People will be told what personal information is collected and why.
- Personal information collected will be of good quality and not too intrusive.
- Personal information will be properly secure.
- People will have access to their own records.
- Use of personal information will be limited and relevant.
- The disclosure of personal information outside the agency will not be allowed
- Respond immediately to any breach of data by:
    - Notifying WSC Management
    - Working collaboratively with WSC to following the Notifiable Data Breach Scheme:
        - Contain
        - Assess
        - Notify
        - Review.

Responsibilities of Educators and Other Team Members:

- Be proactive in fulfilling the requirements of this service policy and related legislative requirements.
- Seek further guidance where required to fulfil your requirements.

- Report any concerns or non-compliance immediately to the Nominated Supervisor or WSC Management.
- Participate in the review of documents and provide constructive feedback to the Nominated Supervisor or WSC Management.
- Ensure personal and confidential information is stored securely using lockable devises or passwords. Do not leave confidential or personal information in accessible areas.
- Only disclose sensitive and private information where required for the provision of education and care, for child protection or where required by law. This includes information shared with third parties such as for Child Care Subsidy or with the regulatory authority.
- Report immediately any breach of personal or confidential information to the Nominated Supervisor or Responsible Person in charge.
- Follow permissions regarding release of information and sharing of photographs.
- Never share or store passwords in an accessible way.
- Conduct private and sensitive conversations in a private location and where possible in the absence of children.

Responsibilities of Families:

- Fulfil responsibilities under this policy and related legislative requirements.
- Understand that the service must take steps as required under legislative requirements and follow advise from recognised authorities.
- Participate in the review of documents and provide constructive feedback to the Nominated Supervisor or WSC Management.
- Discuss any questions with the Nominated Supervisor or Responsible Person in charge.
- Ensure personal information, including any restrictions to persons under a court order are updated regularly.
- Provide permission to display health information such as allergies or life-threatening medical conditions for all educators and visitors to view to protect the health and safety of each child

COMMUNICATION

- Educators and Families will have access to this policy at all times.
- Information will be included in induction for new educator and be included in service handbooks
- Educators and families will be provided with opportunities to be involved in the review of this policy.
- Educators and families will be provided with information from this policy at the time of employment and orientation.
- Changes to this policy and procedure document will be shared with families and educators.

ENFORCEMENT

The Failure of any person to comply with this policy in its entirety may lead to:

- Termination or modification of child enrolment
- Restriction of access to the service
- Performance management of an employee which may lead to termination

RELATED POLICIES AND FORMS

- Information Technology Policy
- Students, Volunteers and Visitors Policy
- Staff Induction Checklist
- Recruitment, Selection and Employment Policy

LEGISLATION, RECOGNISED AUTHORITIES AND SOURCES

The following documents were considered in the development of the Policy:

- *"Guide to the National Quality Framework"* Australian Children's Education & Care Quality Authority September 2020
- *Education and Care Services National Law Act 2010 (version February 2021)*
- *Education and Care Services National Regulations* (version Oct 2020)
    - *168 Education and care service must have policies and procedures*
    - *170 Policies and procedures to be followed*
    - *171 Policies and procedures to be kept available*
    - *172 Notification of change in policies or procedures affecting ability of family to utilise service*
    - *181 Confidentiality of records kept by approved provider*
    - *183 Storage of records and other documents*
- *National Quality Standards*
    - *1.3.3 Information for families*
    - *2.2.2 Health practices and procedures*
    - *2.2.3 Child protection*
    - *4.2 Professionalism*
    - *QA6 Collaborative partnerships with families and communities*
    - *QA7 Governance and Leadership*
- *Office of the Australian Information Commissioner (OAIC) – Australian Government* https://www.oaic.gov.au/
- ACSC Australian Cyber Security Centre https://www.cyber.gov.au/

CEO DISCRETION

Where applicable, the CEO can apply his discretion as to the enforcement of the procedures outlined in this policy.

REVIEW OF POLICY

This policy remains in force until amended or repealed by resolution of Council. This document will be review biannually or as required.

RECORD OF AMENDMENTS and ADOPTIONS			
DATE	**REVISION NO**	**REASON FOR AMENDMENT**	**ADOPTED BY COUNCIL**
October 2021	V1.0	Prepared for Council Adoption	Month YYYY