SANCTUARY
early learning adventure

# CONFIDENTIALITY & PRIVACY POLICY

## POLICY GOAL

To protect 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.

## RATIONALE

We are committed to ensuring the confidentiality of a range of records under state and federal legislation. 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***

*The approved provider of an education and care service must ensure that information kept in a record under these Regulations is not divulged or communicated, directly or indirectly, to another person other than—*

*(a) to the extent necessary for the education and care or medical treatment of the child to whom the information relates; or*

*(b) a parent of the child to whom the information relates, except in the case of information kept in a staff record; or*

*(c) the Regulatory Authority or an authorised officer; or*

*(d) as expressly authorised, permitted or required to be given by or under any Act or law; or*

*(e) with the written consent of the person who provided the information."* [1]

We are committed to protecting personal information. This Policy embodies this commitment and applies to personal information collected by our service. 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.

***What is personal information?***

Personal information is broadly defined under the Privacy Act as information or an opinion about a person, which identifies that person or would allow his or her identity to be reasonably ascertained. Some examples of personal information include names, addresses, phone numbers, photographs and email addresses.

[1] "*Education and Care Services National Regulations*", Ministerial Council for Education, Early Childhood Development and Youth Affairs (Feb 2018)

***Information we collect and how that information is used***

We collect personal information in order to comply with state and territory legislation and only use personal information for the purposes for which it was provided and for directly related purposes (unless otherwise required by or authorised under law).

Information is only collected if it is required for the functions of the organisation. All information must be collected 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. Information that is public record or publicly accessible such as from social media sites may also be collected where it relates to the employment of a team member or the enrolment of a child/family at the service. Examples of some types of information we collect, includes, but is not limited to;

- Specific information about educators, families and children as listed under the National Regulations 2011.
- Information about children's learning, development and participation in programs and activities.
- Contact details
- Immunisation details
- Records of sensitive data such as TFN's, Health Care and Concession Cards, birth certificates, photo identification where required to verify a person's identity.
- Bank and payments information

***Access to and alteration of records containing personal information***

When you provide personal information, you are allowed access to your personal information and may correct the information if it is inaccurate (subject to restrictions on such access/alteration of records under the applicable provisions of any law of the Commonwealth).

***Disclosure***

We will only disclose personal information for the purpose it was collected or as reasonably related to the business. We may disclose personal information about you or your child to third parties associated with the provision of care, the operation of our business or the health, safety and wellbeing of your child, this may include; but is not limited to; public health units, child protection agencies, regulatory authorities, banking and financial institutions collecting fees on our behalf, debt collection agencies (only where a debt is unable to be recovered), technology service providers and legal advisors. We share your information through our CCMS software to directly link to Human Services for the purpose of applying child care subsidies and any associated benefits or claims. We do not disclose your information to direct marketing agencies.

***Storage of Data***

We are committed to ensuring your personal information is stored and disposed of in a secure manner. Personal enrolment information, including banking information, is stored electronically under password protected software packages with limited access to authorised persons only. Credit card details are encrypted in this package. Paper copies are kept in locked cabinets with limited access and when destroyed are done so in a manner to protect information such as shredding.

***Questions and Concerns***

If you have any questions about your privacy and confidentially you should speak firstly with the Nominated Supervisor and follow the grievance procedure displayed in the foyer.

***"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. The guidelines are not prescriptive, as each APP entity needs to consider how the principles apply to their own situation (in terms of operations, data management, IT platforms, etc).*

*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.*

***New requirements under the Privacy Act as of February 2018***
*The Privacy Act was amended in February 2017, with the changes due to take effect on* ***February 22, 2018****.*

*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 (ie. data leaks) that are "likely" to result in "serious harm."*

***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."*[2]

**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"*[3]

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

[2] Information factsheet provided by Australian Childcare Alliance December 2017
[3] "Identifying eligible data breaches" Office of the Australian Information Commissioner (accessed on-line April 2018) 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*" [4]

*"Cyber attacks are the fastest growing crimes throughout Australia and across the world. The Australian Cyber Security Centre's 2016 Cyber Security Study reported that 90% of Australian businesses have experienced a security breach or threat. Even large corporations with up to date software and protections in place have fallen victim to cyber-attacks. There have been successful attacks within large financial institutions, IT and software development companies, governments and large hospitals. Examples include; Uber, Facebook, Ashley Maddison, Australian Red Cross and the Australian Bureau of Statistics to name a few.*

***Protecting your business from a cyber-attack***
*It's important for all businesses to understand that protecting themselves from a cyber-attack is not just an IT or management issue. This is a whole business issue that all staff need to be aware of so they can contribute to the risk management processes and systems. If any staff fail to adhere to the strategies put in place, regardless of that staff member's role and level of responsibility, this can put the business at risk.*

***Tips for 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*
*• Use the resources and information found on www.staysmartonline.gov.au"*[5]

[4] "Assessing a suspected data breach" Office of the Australian Information Commissioner (accessed on-line January 2018) 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

## IMPLEMENTATION

- The Service Provider, Nominated Supervisor and all educators must ensure that records and information are stored appropriately to ensure confidentiality and in accordance with legislative requirements.
- Records will be kept in such a way that restricts unauthorised access.
- Information will be collected as required under section 181 of the Education and Care Services National Regulations
- Families will be given access to all information kept at the service in relation to themselves and their children except where documents are protected in a court order or other relevant document.
- Nominated Supervisors should ensure they are aware of the current legislative requirements.
- Where applicable forms will advise of the reason for the collection of the information and the intended use.
- Permission will be sought from families for the use of photographs both at the service and externally.
- No person is authorised to give out information relating to any child or adult at the service including educators without the permission of that person (or guardian in the instance of a child). This excludes instances where information is required to be shared for medical emergencies or under legislation.
- The Centre will obtain parent/guardian permission before disclosing a child's personal and sensitive information to a professional attending the program for the specific purpose of providing a service to a child. This includes early intervention teachers, speech therapists, occupational therapists and doctors.
- Information relevant to the provision of care to a child as provided by parents or other persons will be shared with educators caring for that child.
- Families are advised that information about children including their names, birthday and photos may be displayed around the service. If families do not wish this to occur, they should notify the Nominated Supervisor immediately.
- The Service Provider, Nominated Supervisor and educators will take all reasonable precautions to ensure personal information that is collected, used and disclosed is accurate, complete and up-to-date. However, the accuracy of that information depends, to a large extent, on the information that is provided by the individuals.
- Individuals will be required to advise our service in writing of any changes that may affect the initial information provided.
- We will take all reasonable steps to protect personal information from misuse, loss, change and unauthorised access/disclosure.
- Government identifiers such Customer Reference Numbers, Health Care Card Numbers, Medicare numbers or Veteran's Affairs numbers will only be used for the purpose for which they were provided.
- We respect the rights of individuals with respect to personal and sensitive information. A higher level of privacy protection applies to sensitive information:
    - Sensitive information relates to information about an individual's religious beliefs, racial or ethnic origin, philosophical beliefs, political opinions, membership of a political persuasion, membership of a trade union, sexual preferences or practices, criminal records or health information.
    - Sensitive information can only be collected with an individual's (or parent's/guardian's) consent to do so.
    - Sensitive information can only be used when informed consent is obtained at the same time the information was collected.

- Educators will conduct confidential conversations in a quiet area away from other children, parents and educators. Such conversations are to be written down and stored in a confidential folder where appropriate.
- The service will provide all staff employed with a Confidentiality Deed and provide induction including confidentiality and use of social media up employment and annually.
- Paper copies will be stored in locked cabinets with limited authorized access.
- The destruction of paper documents containing personal information will be done in a way that protects personal sensitive information such as through shredding.
- The unauthorised use of family or educator contact details collected by service for use in the provision of education and care will be considered a breach of this policy and the Confidentiality Deed and appropriate steps will be taken to protect the use of this information.
- The service will 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.

**At our Service we 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.

**Steps to protect sensitive written information**

- Computers storing images of children and any other sensitive information must be password protected. Computers should be set to require a password after a short period of inactivity and must be shut down after each use and each evening requiring a password to reactivate the next time it is used.
- Software used to process payments must store credit card information in a secure manner
- Any forms which include bank account details and credit card information after being entered into payment software should have credit card information protected including concealing the CCV and all digits excluding the first 4 and last 4 digits.
- Where sensitive information such as identification, birth certificates, concession cards and credit cards are collected for the purpose of providing education and care, the copy made at the service should have the word COPY written on it or stamped or marked in a way that does not conceal relevant information but makes the document unable to be copied and used in an unauthorized way.
- Where documents are scanned into computers the original should be securely disposed of such as using a shredding machine.
- Where documents are stored electronically the Approved Provider should take the relevant steps to protect this information from unauthorized use.
- In the event of suspected data breach the Approved Provider must seek the guidance of information on the Office of the Australian Information Commissioner website to determine the best course of action to be taken including assessing and possibly reporting a notifiable breach. Notifiable breaches must be investigated and reported using the Notifiable Data Breach Form located at https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB

**Steps taken to protect from Cyber Attack**

- Staff only have access to what they need, universal access to programs and documents are not universal
- When staff leave the business, the Nominated Supervisor or Approved Provider must remove all access and permissions immediately
- Passwords to centre data must be strong and not shared with unauthorised persons, individual logs in should be used for all programs
- Nominated Supervisors should ensure all data and information is backed up regularly and store in a safe and secure way.
- Educators should not click on any links or documents in emails from an unknown person or with email addresses which do not match the business name.

## COMMUNICATION AND CONSULTATION

- Upon enrolment families will be advised of the purpose of collecting information and its intended use.
- Educators and families will have access to this policy at all times.
- Educators and families will be provided with opportunities to be involved in the review of this policy.
- Forms collecting personal information will advise of the purpose of collecting information and its intended use.
- This policy will be provided to educators upon employment and to students/volunteers upon commencement.

## RELATED FORMS AND DOCUMENTS

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

## SCOPE AND ENFORCEMENT

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

- Termination of Child Enrolment
- Performance Management of an employee which may lead to Termination

## RECOGNISED AUTHORITIES AND DOCUMENTS WHICH GUIDE POLICY


- "*Education and Care Services National Regulations*", Ministerial Council for Education, Early Childhood Development and Youth Affairs (Feb 2018)
- "The Privacy Act" Australian Government (1988)
- Officer of the Australian Information Commissioner, Australian Government website (accessed on-line April 2017) http://www.oaic.gov.au/
- "Credit and Debit Card Payments" Australian Government (accessed on-line January 2018) https://www.business.gov.au/info/run/finance-and-accounting/accounting/payments-and-invoicing/credit-and-debit-card-payments
- "Privacy Fact Sheet 17 – Australian Privacy Principles" Australian Government Office of the Australian Information Commissioner (accessed on-line January 2018 https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.pdf )

- "Identifying eligible data breaches" Office of the Australian Information Commissioner (accessed on-line January 2018) https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/identifying-eligible-data-breaches#key-points
- Information factsheet provided by Australian Childcare Alliance December 2017
- "Privacy Amendment (Notifiable Data Breaches) Act 2017 (accessed on-line January 2018) https://www.legislation.gov.au/Details/C2017A00012
- "Assessing a suspected data breach" Office of the Australian Information Commissioner (accessed on-line January 2018) https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/assessing-a-suspected-data-breach
- Notifiable Data Breach Form Office of the Australian Information Commissioner (accessed April 2018) https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB
- *"Business Cyber Security Obligations"* Guild Insurance Jan 2018


**DATE CREATED:** July 2018

**REVIEW DETAILS:**

| Review Date | Next review due |
|---|---|
| September 2024 | September 2025 |