EIKOH SEMINAR AUSTRALIA PTY LTD

PRIVACY & CONFIDENTIALITY POLICY

Statement - To protect the privacy rights of the child and their family and the staff and their family. This policy is to ensure that families and staff understand who has access to records and information obtained within the service.

Introduction

Our education and care service recognizes and respects the importance of privacy and confidentiality as an individual right and a basis for building partnerships. Our service requires personal information from families to provide appropriate and responsive care. This policy has been developed to comply with the Australian Privacy Principles (APPs)(2014) and pursues the highest standard in the protection and preservation of privacy and confidentiality.

Goals

We will:

- Maintain private and confidential files for educators and staff, children and their families. We will develop systems for the appropriate use, storage and disposal of records.

- Ensure the information in these files is used only for the education and care of the child enrolled in the service, and only shared with relevant or authorized people as defined within authorisations for the Education and Care Services National Regulations.

Strategies

Our education and care service aims to meet these goals through the adoption of this specific Privacy and Confidentiality policy and our Privacy Collection statement which will guide our practices in this area.

The Approved Provider will:

Collection of Information

- Ensure that each family, staff, volunteers and student and committee member is provided with a privacy collection statement upon enrolment, that includes details about how they can access their personal information, have this corrected as needed, make a complaint about a breach of privacy, if one occurs.

- Ensure each staff member, committee members, volunteers and student information is correct in personnel and other files. This includes information on qualifications, WWCC, criminal history checks, staff entitlements, contact and emergency information, health and immunisation information, and any relevant medical and legal information this would include any other relevant information collected by the service.

- Ensure that information collected from families, educators, committee members and the community is maintained in a private and confidential manner at all times.

- Ensure that such information is not divulged or communicated (directly or indirectly) to another person other than the ways outlined as appropriate in the Education and Care Services National Regulations, 181, which says information can be communicated:

    - To the extent necessary for the education, care or medical treatment of the child;
    - To the parent of the child to whom the information relates (except for information in staff records);
    - To the regulatory authority or an authorized officer;
    - As authorized, permitted or required to be given by or under any act or law; and
    - With written consent of the person who provided the information.

- Ensure families are informed upon enrolment how images/photographs of their children will be used within the Centre. Permission from families will be gathered for their child's image and photos engaged in learning experiences to be used within our Centre App.

- Provide families with information on the Complaints procedure if any privacy or confidentially procedure has been breached. Individuals can make a complaint to the Approved Provider if they believe there has been a breach of their privacy in relation to the Privacy principles. The breach will be assessed by the Approved Provider within 14 days. Where the information collected is incorrect, the information will be

corrected. Where a serious breach of privacy is found, appropriate actions will be negotiated between the Approved Provider and the individual to resolve the situation, in line with the Complaints procedure.

- Will ensure information provided by families, staff and committee members is only used for the purpose it was collected for.

The Nominated Supervisor will:

- Ensure each family's information is correct in enrolment records. This includes information on immunisation updates, contact details of family and emergency contact information, children's developmental records, Family Assistance information, and any medical or legal information – such as family court documentation – required by our education and care service. This would include any information required to be recorded under the National Law and Regulations, the Family Assistance Law other relevant information collected to support the enrolment of a child.

  Provide families with details on the collection of personal information collected:

  This information will include:

  - The types of information collected by our education and care service;
  - The purpose of collecting information;
  - What types of information will be disclosed to the public or other agencies; and when and why disclosure may occur;
  - How information is stored at the service;
  - Approaches used to keep information secure;
  - Who has access to the information;
  - The right of the individual to view their personal information;
  - The length of time information needs to be archived; and
  - How information is disposed.
  - How photos of the children will be used within the App.

- Will ensure information provided by families and staff is only used for the purpose it was collected for.

Storage of information

- Ensure that education and care service records, personnel records, CCS information and children's and families information is stored securely reducing the chance of unauthorized access, use or disclosure and remains private and confidential within the education and care environment at all times.

Access to Information

- Families will have access to their child's learning and development records through the Centre's App unless this is not possible due to custody or child protection orders.

- Will ensure that information kept is not divulged or communicated, directly or indirectly, to anyone other than:

  - Medical and developmental information that is required to adequately provide education and care for the child;
  - The Department of Education and Communities, or an authorized officer; or
  - As permitted or required by any Act or Law.

- Individuals will be allowed access to their personal information as requested. Individuals must request this information in writing from the Nominated Supervisor. Authorised persons may request to view any information kept on their child.

- Information may be denied under the following conditions:
  - Access to information could compromise the privacy of another individual;
  - The request for information is frivolous or vexatious; and
  - The information relates to legal issues, or there are legal reasons not to divulge the information such as in cases of custody and legal guardianship.

Educators will:

- Maintain children's information and store documentation according to policy at all times.

- Not share information about the education and care service, management information, other educators or children and families, without written permission or legislative authority.

- In keeping with the Early Childhood Australia (ECA) Code of Ethics (2008), the Education and Care Services National Regulations and the Privacy Legislation, educators and staff employed by our education and care service are bound to respect the privacy rights of children enrolled and their families; educators and staff and their families and any other persons associated with the service. Educators will sign a Confidentiality Statement as it relates to privacy and confidentiality of information.

Privacy Online

Introduction:

Websites, social media sites, the Centre's App developed by OWNA Corp Pty Ltd and families can provide information to potential clients on what an organisation offers. A Website maintained by the education and care service can support families to make informed decisions about education and care and find out more about if a particular education and care service will suit their requirements. Families are also able to gain contact information or request further information through emails. Social media and the Centre's App may be utilised to support enrolled families to communicate and share information.

Goals:

Our Centres website App (developed by OWNA Corp Pty Ltd) is maintained to inform families about the activities and the services provided by the organisation. Our centre respects the privacy of educators, children and families. Our centre seeks to keep all records private and confidential and maintains records according to the National Privacy Principles and the Education and Care Services National Regulations 2011. Through our staff manual guidelines are set for educators in regard to social media participation connected with their work as early childhood educators.

Strategies:

The Nominated Supervisor will:

- Ensure that no confidential information can be gained from our centres website. Individuals and services are not obliged to give personal information through the website. However, if an individual chooses to provide information to service via email, that information will remain confidential.

- Ensure that information gained via email can only be used by administration staff or management to contact a person, offer or send information about the service and to request feedback on the website or our centre.

- Ensure that information gained about users from the website will only be used for statistical research for the education and care service to ascertain future development of the website. This information will not be available to any other organisations:

    - IP address, the date and time of the visit
    - pages accessed and documents downloaded on this site
    - search terms used
    - previous site visited
    - network providers name
    - any cookies that the browser has presented to the server
    - the browser, operating system and various plugins that were used in visiting the site.

- Encourage families and educators to give feedback on the website and how it can be improved to meet the needs of the community.

- Not disclose or publish any information related to educators, children or families without written consent from that individual or their family.

- Utilise guidelines set in our staff manual for educators regarding their participation with families currently connected with the centre on social media sites such as Facebook and Twitter.

Centre App

In 2019 we developed an App in conjunction with OWNA Corp Pty Ltd. The aim of the App is to cut down on the amount of paper used and stored by the centre and to communicate more effectively to families about their child's day. As a part of our commitment to privacy and ensuring our commitment to child protection only authorised persons will have access to information contained within the App. All authorised persons will have a Working with Child Check.

Information from the App and personal records are kept in accordance with our retention of records policy on OWNA's Server and our company server stored at our head office. The App is available to download via the App store – only families currently enrolled in the centre will be able to access this App. A link will be sent to the families to download. Families permission will be sought to publish their child's image through the App. These photos will be used to demonstrate the children's learning. Families who do not which their child's image to be available to other families will still be included within the App. That child's photos will still be included in the App however will not be apart of group images of other children and the images will only be visible to that child's family – a lock feature can be used to ensure this happens.

Families will have access to the App while enrolled at the centre. Upon leaving the centre the family will be able to access the App for four (4) weeks from the time leaving notice is received by the Centre Director before the child's account becomes inactive, as per the permission letter.

Families will be able to post to the App via their login – this will go to draft mode and educators will push through their post on the next business day.

Breaches of Personal Information

The Approved Provider or Nominated Supervisor will implement the Service's Data Breach Response Plan and notify individuals and the Australian Information Commissioner (the Commissioner) if personal information is lost (hard copies or electronic), accessed or intentionally/unintentionally disclosed without authorisation, and this is likely to cause one or more persons serious harm.

Data Breach Response Plan

Employees must notify the Approved Provider or Nominated Supervisor about a breach or suspected breach of personal data as soon as they suspect the breach or become aware a breach has occurred. The approved Provider or Nominated Supervisor will:

- Quickly assess the situation to decide whether or not there has been a breach. This assessment must be completed within 30 days but given the potential for serious harm to individuals, should be completed as soon as possible.
- Record the nature of any data breach, and the steps taken to immediately contain the breach where possible and ensure it does not happen again. If necessary they will contact external experts for advice and guidance, for example on cybercrime (hacking) and information technology security measures like access, authentication, encryption and audit logs
- Notify the commissioner and the individuals where there is a risk of serious harm after a data breach
- Liaise with their insurer to determine whether the insurance policy covers data breaches and any steps they need to take
- Evaluate the effectiveness of their response to the data breach and implement improvements to the Plan if required after all notifications, records and remedial action are taken.

Serious harm

The Approved Provider or Nominated Supervisor will decide whether serious harm of a physical, s\psychological, emotional, financial or reputational nature is likely once fully informed about the type and extent of the breach. The will consider the type and sensitivity of the information, they type of security protecting the information if any (e.g. encryption) and how likely it is the information will be used to cause harm to individuals. Examples of the kinds of information that may increase the risk of serious harm include sensitive information like an individual's health records, documents commonly used for identity fraud e.g. Medicare card, birth certificates and financial information.

The Approved Provider or Nominated Supervisor will also consider how long the personal information has been accessible because serious harm is more likely the longer it has been since the data breach.

Where a data breach occurs, there may be not always be a risk of serious harm. This may be the situation, for example, if a trustworthy person or organisation who has received personal information in error confirms they have not copied, and have permanently deleted the information, or where expert advice states it's unlikely encrypted data can be accessed.

Where they are satisfied there is no risk of serious harm, the Approved Provider or Nominated Supervisor are not required to notify individuals or the Commissioner about the breach. They may choose to advise the individuals concerned about the breach and the action taken. The Approved Provider or Nominated Supervisor will however keep appropriate records about the breach.

Notifying the Commissioner

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will prepare a Statement for the Commissioner which includes the name and contact details of the Approved Provider or Nominated Supervisor, a description of the data breach (including date occurred and detected and who obtained information), the type of information involved (why it may cause serious harm), and the steps individuals at risk of serious harm should take in response to the breach (e.g. steps to request new Medicare card or credit card). The Approved Provider or Nominated Supervisor will get specialist advice about the recommended steps if required. They may use the Notifiable Data Breach Form available online from the Office of the Australian Information Commissioner to notify the Commissioner.

Notifying Individuals

Where there is a risk of serious harm after a data breach, the Approved Provider or Nominated Supervisor will notify individuals about the breach as soon as possible using the most appropriate communication methods for the individuals concerned e.g. a telephone call, SMS, physical mail, social media posit, or in-person conversation. The information provided is the same as that required for the Commissioner. It might also explain steps the Service has taken to reduce the risk of harm to individuals. The Approved Provider or Nominated Supervisor may notify everyone whose personal information was part of the breach or only those individuals at risk of serious harm.

Source: **Early Childhood Australia**
Privacy Act 1988
Education and Care Services National Regulations 2011:
National Quality Standards
Community Child Care Co-operative (NSW)
Dated: **July 2019**

Privacy Collection Statement

Our service is committed to maintaining all personal information provided by its children, families, staff, management, volunteers, students and community in accordance with our Privacy policy and the Australian Privacy Principles.

Each family, staff, volunteers and student is provided with a privacy collection statement upon enrolment or commencement of employment.

This statement outlines the type of personal information collected by our service and how information is acquired, used and shared. We will not sell personal information to any third parties. See our full Privacy and Confidentiality policy for detailed information.

What is person information? How is it collected and why?

What information is collected?	How we collect information?	Why we collect this?
Medical information, health and immunisation	• Employment form • Enrolment record • Immunisation history statement • Health care cards – Medicare and health fund information • Accident, Illness and Injury forms	To ensure the health and safety of every child and as a requirement under *Family Assistance Law* and the *NSW Public Health Act 2010*.
Income and financial details, includes credit card and banking information	• Employment form • Enrolment record • Fee payment and purchases • Tax File Number	For the provision of the education and care service and as required under Family Assistance legislation and as per Funding Agreements with the Department of Education and Communities.
Contact details of family and emergency contact information	• Enrolment form • Employment record • Updated details form	Required under the *Education and Care Services Regulation*.
Children's developmental records	• Observations • Assessment of children's learning • Programming documents • Communications with families	Required under the *Education and Care Services Regulation* and to provide a high quality education and care service.
Family Assistance information	• Enrolment form • Employment record • CCMS	Required under the Family Assistance legislation and under employment legislation under Income Tax legislation.
Legal information	• Enrolment form • Employment record • Court orders or AVOs	Required under the *Education and Care Services Regulation*.
Employment, marital status and nationality	• Enrolment form • Employment record	Required under employment legislation and to provide priority of access under commonwealth and state legislation.
Qualifications	• Employment record	Required under the *Education and Care Services Regulation*.
WWCC, criminal history checks	• Employment record • Originals of documents	Required under the *Education and Care Services Regulation*.
Staff entitlements	• Payroll records • Tax File Number	Provision of entitlements.

What information is collected?	How we collect information?	Why we collect this?
Any information required to be recorded under the National Law and Regulations, the Family Assistance Law other relevant information collected to support the enrolment of a child	• Enrolment form • Employment record • Complaints records	Required under appropriate legislation.

Personal information is information that personally identifies an individual, such as a name, residential or email address and includes information relevant to the enrolment process, credit card information, billing records, documentation of a child's learning and development, and recorded information regarding complaints.

Publicly available information, such as information on a public website profile is not considered personal information.

Our service only collects personal information when individuals specifically and knowingly elect to provide this, such as when individuals enrol a child in the service, pay fees and provide health or family information to support the inclusion of a child.

This service complies with the Payment Card Industry Data Security Standards (PCIDSS) when handling credit card transactions and securely stores all credit card information for credit card payment/eftpos payments in accordance with the Fees policy.

Direct Communications

Our service uses individual's personal information to send information by post, email or telephone. Individuals are provided with an opportunity to elect not to receive such information upon enrolment or through written notification to the service.

What happens with personal information?

This service will strive to let individuals know how any personal information will be used at the time of collection. Individuals will be asked if personal information can be used to establish contact with them regarding other aspects of organizational business. This service will not sell or trade individuals' personal information to other third parties.

This service collects and uses personal information generally to provide individuals with the information and the services they request, to provide appropriate and relevant information pertaining to the education and care of a child/ren, and to continue to improve service quality.

Where is personal information stored?

Personal information is stored in a safe and secure manner, using locked filing cabinets or a password protected database and computer. Information is backed up electronically and securely stored. Data will not be altered or destroyed except in extraordinary circumstances.

Hard copy information is stored at the service, which is secured to prevent entry by unauthorized people. Any personal information not actively being used may be archived, in accordance with regulatory requirements.

Personal information will remain on the service database indefinitely until personally advised by a customer that information is to be removed, unless information has been archived or destroyed at an earlier date in accordance with privacy law and regulatory requirements.

Access and updating personal information

Individuals may ask to access, update or delete personal information held about them at any time. Reasonable steps will be taken to verify an individual's identity before granting access, making any corrections to, or deleting information. If a customer wishes to make a complaint, please refer to the Complaints Procedure.

Individuals requiring access to, or wanting to update personal information, can contact the service via telephone or email.