Centre Policy Manual

Privacy Policy

Rationale:

To ensure that all personal and individual information received is used for the purpose for which it is obtained and to ensure that the privacy Act 2020 is adhered to.

Objectives:

- To adhere to the Information Privacy Principles outlined in the Privacy Act 2020
- To protect the rights of all individuals in accordance with the Privacy Act 2020.
- To assist staff in understanding their obligations in accordance to the Privacy Act 2020.
- To ensure the storage of personal information is kept safe on Centre premises, online, and in the Support Office.
- To ensure that immediate action is taken in the event of any breach of privacy.

Information Privacy Principles - Privacy Act 2020

The Privacy Act has 13 Information Privacy Principles (IPPs) which outline how personal information is collected, stored, accessed, corrected, used and disclosed. An overview of the IPPs can be read here: https://www.privacy.org.nz/news-and-publications/guidance-resources/a-quick-tour-of-the-privacy-principles/.

In summary, the IPPs are:

1. Only collect the information you need
2. Where possible, get the information directly from the person
3. Be clear about what the information will be used for
4. Use fair and reasonable ways of collecting information
5. Keep information safe
6. Let people access information about themselves
7. Correct information if the person thinks it is wrong
8. Make sure information is accurate before you use it
9. Only keep information as long as you need it
10. Only use the information for the purpose you collected it
11. Only share personal information if you have a good reason
12. Only send personal information overseas, if the agency outside of New Zealand, if there are similar safeguards to those in the Privacy Act.
13. Only use individual identifiers if it is clearly allowed.

Centre Leadership Responsibilities:

- The professional Leader will be responsible for ensuring the privacy of information within the Centre or will delegate the responsibility to a Person Responsible.
- The Professional Leader/Person Responsible will undertake the training provided by the Privacy Commissioner's office (see: https://www.privacy.org.nz/further-resources/online-privacy-training-free/). The certificate of completion will be uploaded to the person's enableHR staff file.

  It is the responsibility of the Professional Leader/Person Responsible to:
  - Ensure the centre complies with the Privacy Act 2020 information privacy principles
  - Handle requests for personal information, including but not limited to, safeguarding children under the Children's Act 2014.

- Work with the Support Office Privacy Officer in relation to investigations
- Ensure staff within the Centre have completed the online PLD training and are familiar with the Privacy Policy
- Monitoring compliance with policies and procedures
- Handling complaints
- Inform the Support Office Privacy Officer of any breaches in privacy, or requests for sensitive information.

Support Office Privacy Officer:

The delegated Support Office Privacy Officer, Allison Sumner Allison.sumner@provincialeducation.co.nz, will be responsible for:

- Ensuring the support office complies with the information privacy principles and Privacy Act 2020
- Handling requests for personal information where applicable
- Handling requests for sensitive information from staff
- Supporting Centres where information requested is of a sensitive nature or where a request for information has been refused.
- Notification of serious breaches of privacy to the Privacy Commissioner and informing individuals concerned.
- Working with the Privacy Commissioner in relation to Investigations.
- Handling complaints

Procedures:

- Personal information is only accessible by authorized personnel and stored in Management's office to ensure safeguard against loss or wrongful disclosure. Breaches of confidentiality will be regarded as serious misconduct (refer to the Team Handbook, Social and Digital Media Policy, Marketing Guidelines Policy, Our Code Our Standards (2017)).
- Personal information pertaining to individuals will not be disclosed to any unauthorised person or persons. Under the Education and Training Act 2020 (section 626) and the Licensing Criteria for ECE services, any government official may request and access any information held by the centre about any child or parent.
- Personal information will only be used for its intended purposes.
- Requests for information will be responded to by the Centre Manager/Privacy Officer within 20 working days of the request being received. Request for information may be refused if Management deems the disclosure of information falls under Section 49 of the Privacy Act 2020:

  An agency may refuse access to any personal information requested if—

(A) the disclosure of the information would—

(i) be likely to pose a serious threat to the life, health, or safety of any individual, or to public health or public safety; or

(ii) create a significant likelihood of serious harassment of an individual; or

(iii) include disclosure of information about another person who—

(a) is the victim of an offence or alleged offence; and

(b) would be caused significant distress, loss of dignity, or injury to feelings by the disclosure of the information; or

(B) after consultation is undertaken (where practicable) by or on behalf of the agency with the health practitioner of the individual concerned, the agency is satisfied that—

(i) the information relates to the individual concerned; and

(ii) the disclosure of the information (being information that relates to the physical or mental health of the requestor) would be likely to prejudice the health of the individual concerned; or

(C) the individual concerned is under the age of 16 and the disclosure of the information would be contrary to the interests of the individual concerned; or

(D) the disclosure of the information (being information in respect of the individual concerned who has been convicted of an offence or is or has been detained in custody) would be likely to prejudice the safe custody or the rehabilitation of the individual concerned.

- Management is responsible for updating changes to personal information.
- Management is responsible for advising staff if/when a child enrolled has no consent to upload photos online.
- Staff are responsible for updating their private information directly with Provincial Education Group Limited (PEGL) Human Resources.
- Personal information will be held on file for 7 years, or for the duration of a staff members employment (whichever is longer).
- Personal information will be disposed of securely when no longer required, to ensure it cannot be retrieved.
- Staff are required to role model high and consistent standards of confidentiality, integrity and professionalism, both personally and/or via social media; this includes but is not limited to any Centre information regarding children, whanau, team or incidents within the Centre.
- Staff will not share any privileged information learnt at work relating to families, management, fellow staff and/or their families with any other person either at work or outside the workplace, with the exception of Management where appropriate.
- Staff will not share information about their renumeration, demonstrating a high standard of professional behaviour and integrity (refer Team Handbook and Employment Agreement)
- Staff will not directly or indirectly make or cause disparaging comments or demonstrate behaviour that brings the Centre into disrepute.
- Staff shall not at any time, or for any reason, whether during the term of employment or after termination, use or disclose to any person, any confidential information relating to their current or past employment.
- Computer passwords will be programmed on to all files marked CONFIDENTIAL and be accessible to authorised personnel only.
- Staff or students in formal ECE training must gain Management's or, where applicable, Parent/guardian consent before conducting any research (observations/photos/records)
- Staff or students conducting research (questionnaires, surveys, and observations) must adhere to the right of confidentiality and privacy when engaging with children and parents as sample groups. Children and their parents' initials are only to be used. Children and parents involved in the research process have the right to access the draft research they took part in. **NB:** both parties have the right to withdraw at any time from the research process.
- Photographs of children will only be posted on social/digital media where written consent has been given by the child's parent/guardian (refer to Enrolment Form).

Managing Privacy Breaches:

- All staff are required to report potential privacy breaches that they become aware of as soon as possible to the Centre Manager or the Support Office Privacy Officer.
- Where a potential privacy breach has been discovered, the centre manager will take immediate steps to contain and assess the situation on an urgent basis.

  A privacy breach, in relation to personal information held by an agency,—
  (a) Means -
  (i) unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or
  (ii) an action that prevents the agency from accessing the information on either a temporary or permanent basis; and
  (b) includes any of the things listed in paragraph (a)(i) or an action under paragraph (a)(ii), whether or not it -
  (i) was caused by a person inside or outside the agency; or
  (ii) is attributable in whole or in part to any action by the agency; or
  (iii) is ongoing.

- The centre will undertake an initial investigation to determine what has happened and take steps to mitigate and/or minimise any harm or potential harm.
- In the event of a notifiable breach, the Professional Leader will inform the Support Office Privacy Officer and/or CEO as soon as practicable after becoming aware of the breach. A notification will be made to the Privacy Commissioner and affected parties.
- A notifiable breach is one that has or is likely to cause serious harm to affected individuals. When determining whether the breach is likely to cause serious harm, the following factors will be considered:

    - The actions that have been taken to reduce the risk of harm following the breach
    - Whether the personal information is sensitive in nature (information about children)
    - The nature of the harm that may be caused to affected individuals
    - The person or body that has obtained or may obtain personal information as a result of the breach (if known)
    - Whether the personal information is protected by a security measure
    - Any other relevant matters.

More information about the Privacy Act and useful resources can be found here on the Privacy Commissioner's website: https://www.privacy.org.nz/. Centre's will be advised of any updates to the Privacy PLD requiring staff to complete further training.

Links: Reg 46 and 47; GMA 2, 10, 12; HS 32; Children's Act (2014), Privacy Act 2020, Children's Act (2014), Section 626 Education and Training Act 2020

Reviewed: May 2021

Next Review: May 2023

See also: Team Handbook
Social and Digital Media Policy
Marketing Guidelines Policy
Complaints Policy & Flowchart
Parents Rights of Entry Policy