Privacy Policy/Tukanga Here

Version 2
Effective Date: 19 May 2023
Next Review: 2026
Document Approver: Chief Executive
Document Owner: Senior Teachers

Applies To | Ko Wai Whakahāngaitia

All staff.

General Principles | Mātāpono Whānui

- To acknowledge the information privacy principles contained in the Privacy Act 1993.
- To ensure Kindergarten Taranaki meets its obligations with respect to the collection, storage, use and disclosure of personal information about employees and about children (and families) attending kindergarten.

Related Procedures or Processes and Documents | Pākanga Tukanga me Pukapuka

Not Applicable.

References | Tohutoro / Huānga ki

Education (Early Childhood Services) Regulations 2008.
Licensing Criteria for Early Childhood and Care Services 2008: GMA-5.
Privacy Act 1993.

Policy Review Cycle | Kaupapa Arotake Hurihanga

This policy will be reviewed every three years and in conjunction with reviews of the related procedures or processes and documents outlined above.

Policy

1. Every person who attends, works at or makes personal or professional contact with Kindergarten Taranaki is entitled to full privacy with regard to personal details, as specified in the Privacy Act 1993.
2. General Principles:

   The Privacy Officer will be the Chief Executive. In the absence of the Chief Executive the Chief Executive may delegate to role to a senior manager.

   The Privacy Officer shall be responsible for:

   - Administration of the Privacy policy and promoting compliance with the information privacy principles (Appendix 1) set out in the Privacy Act, 1993.
   - Receiving and promptly actioning requests made pursuant to the Act for disclosure of personal information held by Kindergarten Taranaki.
   - Working with the Commissioner in relation to investigations conducted pursuant to Part VIII of the Privacy Act, 1993.
   - Otherwise ensuring compliance with provisions of the Act.

3. At the kindergarten level the Head Teachers shall act as a Privacy Officer. They are responsible for ensuring:
    - Information is collected for the purposes it was collected for.
    - Personal information is securely stored.
    - Information collected is accurate.
    - Making available to a person information held about them.
    - Contacting the Chief Executive in the event of any suspected breach of this policy.
4. Complaints alleging breaches of privacy are to be directed to the Privacy Officer.
5. Personal information shall not be collected unless the collection is necessary for a lawful purpose.
6. Where personal information is collected it will be collected directly from the person concerned or in the case of children from the person who is enrolling the child.
7. Where information is collected from an individual, that person shall be made aware that the information is being collected, why it is being collected, how it will be used, the consequences of not providing it and the individual's right to have information corrected.
8. All personal information held in Kindergarten Taranaki's office or at a kindergarten will as far as is reasonably possible be protected against loss or unauthorised use, modification or disclosure.
9. Every person is entitled to seek confirmation of the accuracy of personal information and to seek its correction if necessary.
10. Kindergarten Taranaki will make available to all staff information regarding the 12 Principles of the Privacy Act.

Employment Information

1. Personal files held on employees shall comprise:
    - Copies of correspondence between Kindergarten Taranaki and the employee.
    - The application for the position currently held and any documentation provided with that application.
    - Copies of qualifications and Teacher Registration Practising Certificate and applications for teacher registration where appropriate.
    - Copies of evidence of professional development such as certificates.
    - Miscellaneous records (e.g. sick leave records).
    - Material compiled for the purpose of promotion, competency proceedings or dismissal.
2. Access to personal files is restricted to the Chief Executive, People and Culture Team members, Senior teacher team and the staff member whose file it is. If an employee wishes to view their file they should contact the Privacy Officer and make a time to do so.
3. Kindergarten Taranaki shall ensure that the personal information it holds is accurate, up to date, complete, relevant and not misleading.
4. Every person is entitled to seek confirmation of whether or not personal information is held, to access that information and to seek its correction. Corrections sought shall be actioned or, where declined, shall be noted in a statement attached to the information.
5. Evaluative material prepared in confidence, as defined in Section 29(3) of the Privacy Act 1993, may be protected from disclosure to the employee concerned.

6. Personal information shall not be kept for longer than is required for the purposes for which it was collected or held.
7. Personal files of staff who have resigned shall be held for such time as is required by relevant statute. Salary and sick leave details shall be retained in case a staff member returns to the employment of Kindergarten Taranaki.
8. Information held regarding former employees shall not be disclosed without their consent, except where the disclosure is made pursuant to a direction of a court order.
9. Unique identifiers shall not be assigned to individuals unless required for the effective functioning of Kindergarten Taranaki. The unique identifier shall not be the same as that assigned by another agency.
10. The gathering of, and access to, information pertaining to investigation of complaints shall be consistent with Kindergarten Taranaki Complaints Procedure.
11. Application forms submitted by unsuccessful job applicants shall be destroyed immediately an appointment is made unless permission is sought and given by the applicant. Comment sought from nominated referees is provided on the basis of confidentiality and detail of these reports shall not be made available to applicants.

Children's records

1. Any information about an individual child is personal information under the Privacy Act 1993 and all principles of the Act apply to it, regardless of the age of the child.
2. Personal information about a child may not be disclosed to a third party without the written permission of the child's parent/guardian unless the Privacy Officer believes on reasonable grounds that the information for that other purpose is necessary to prevent or lessen an imminent threat to:
    - Public health or public safety; or
    - The life or health of the individual concerned or another individual.
    - It has been requested under a Government statute.
3. Personal information may be disclosed to schools to ensure the best interest of the child are maintained – refer Privacy Act 1993, Part 54, Clause b.
4. Schools may be provided with statistical information, which does not identify individuals.

Procedures

Adult

Kindergarten Taranaki staff will ensure that:

1. Information about the person is collected directly from that person (e.g. Must only contact people whom the applicant has put down as a referee).
2. Explanations are given about what the information is going to be used for and who it will be shared with.
3. Information is only used for a lawful purpose.
4. Only information relevant to the position is collected.

5. Information is stored in locked cupboards to guard against loss or wrongful disclosure.
6. Only staff whose job directly relates to the information has access to it.
7. Information is returned to applicants.

Children

Kindergarten Taranaki staff will ensure that:

1. Information gathered on the Enrolment and Attendance records that are required to be kept for 7 years are secured away from public access and kept dry and secure.
2. Information collected on children is only used for the purpose that it was obtained for.
3. The enrolment form will include information for parents about why it is collected.
4. Only people whose jobs directly relate to the information should have access to it.
5. Information on an enrolled child is shared only with others who need it to effectively carry out their duties related to that child, and parent consent has been obtained to share the information.
6. If the parent/guardian does not consent to the disclosure of any or all of the information, this will be clearly marked (e.g. written in capitals and highlighted) on that child's records to safeguard against accidental disclosure.
7. Information on vulnerable children will be shared following the guidelines in appendix 2.
8. Information on the Privacy of the Ministry of Education ELI Information collection system and Privacy are detailed in Appendix 3.
9. If consent has been obtained the information should be delivered in such a way that unnecessary personal information belonging to that child or others is not accidentally disclosed e.g. blocking out unnecessary information or the children's names.
10. Children's personal information can be given only to the child, the child's legal guardians and to the people granted consent on the enrolment form.
11. If you are at all uncertain, it is best to contact a legal guardian of the child to ask if the information requested can be given to the person/agency asking for it, or if they would like to contact the person/agency directly. If you are still concerned or unsure seek clarification from the Privacy Commissioner.
12. Parents/guardians have equal rights to their child's information unless there is a court order in place that prohibits access to a parent.

In our day-to-day workings with children, for the good of these children, these consent issues may seem obvious. But privacy is a concept that covers a vast area and means a variety of things to different people. We must be careful that we do not make assumptions regarding the children in our care that may offend, humiliate, embarrass or endanger the child or their family.

The following information will be displayed in each kindergarten and at Kindergarten House.

The Privacy Officer is _____

It is their responsibility to:

- Use information collected for the purpose it was collected for
- Ensure personal information is securely stored
- Ensure information collected is accurate

- Make available to a person information held about them

Appendices

Appendix 1 - Information Privacy Principles.

https://privacy.org.nz/news-and-publications/guidance-resources/information-privacy-principles/ includes poster.

Appendix 2 - Privacy Commission recent guidelines on sharing information about vulnerable children.

https://privacy.org.nz/how-to-comply/sharing-information-about-vulnerable-children/

Appendix 3 - Privacy requirements around ELI are set out quite well on the ELI website:

http://eli.education.govt.nz/eli-privacy/privacy-information/

http://eli.education.govt.nz/questions-and-answers/information-and-privacy/

ECE Lead guidance on privacy policies for ECE services:
http://www.lead.ece.govt.nz/ManagementInformation/EstablishingAnECEService/EstablishingACentreBasedService/PoliciesProceduresProcesses/DevelopingPolicies/Privacy.aspx

Appendix 1 - Information Privacy Principles And Poster

At the core of the Privacy Act are 12 information privacy principles that set out how agencies may collect, store, use and disclose personal information.

The Privacy Act uses the term "agency". An agency is any individual, organisation or business, whether in the public sector or the private sector. There are a few exceptions such as MPs, courts, and the news media. Generally, though, if a person or body holds personal information, they have to comply with the privacy principles. See the Privacy Act, section 2, for the full definition of "agency".

"Personal information" is any information about an individual (a living natural person) as long as that individual can be identified.

The privacy principles

The 12 principles of the Privacy Act are:

1. Purpose of collection of personal information
2. Source of personal information
3. Collection of information from subject
4. Manner of collection of personal information
5. Storage and security of personal information
6. Access to personal information
7. Correction of personal information
8. Accuracy etc of personal information to be checked before use
9. Agency not to keep personal information for longer than necessary
10. Limits on use of personal information
11. Limits on disclosure of personal information
12. Unique identifiers

Principle 1 - Purpose of collection of personal information

Personal information must not be collected unless:

- The collection is for a lawful purpose connected with a function or activity of the agency Collecting the information; and
- It is necessary to collect the information for that purpose.

Principle 2 - Source of personal information

Personal information must be collected directly from the individual concerned.

The exceptions to this are when the agency collecting the information believes on reasonable grounds that:

- The information is publicly available; or
- The individual concerned authorises collection of the information from someone else; or
- The interests of the individual concerned are not prejudiced; or

- It is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or
- Complying with this principle would prejudice the purposes of collection; or
- Complying with this principle would not be reasonably practical in the particular case; or
- The information will not be used in a form that identifies the individual; or
- The Privacy Commissioner has authorised collection under section 54.

Principle 3 - Collection of information

When an agency collects personal information directly from the individual concerned, it must take reasonable steps to ensure the individual is aware of:

- The fact that the information is being collected
- The purpose
- The intended recipients
- The names and addresses of who is collecting the information and who will hold it
- Any specific law governing provision of the information and whether provision is voluntary or mandatory
- The consequences if all or any part of the requested information is not provided; and
- The individual's rights of access to and correction of personal information.

These steps must be taken before the information is collected or, if this is not practical, as soon as possible after the information is collected.

An agency is not required to take these steps if they have already done so in relation to the same personal information, or information of the same kind, on a recent previous occasion.

It is also not necessary to comply with this principle if the agency collecting the information believes on reasonable grounds that:

- Collection is already authorised by the individual concerned; or
- It is not prejudicing the interests of the individual concerned; or
- It is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or
- Complying with this principle will prejudice the purposes of collection; or
- Complying with this principle is not reasonably practical in the particular case; or
- The information will not be used in a form in which the individual concerned is identified.

Principle 4 - Manner of collection of personal information

Personal information must not be collected by:

- Unlawful means; or
- Means that are unfair or intrude unreasonably on the personal affairs of the individual concerned.

Principle 5 - Storage and security of personal information

An agency holding personal information must ensure that:

- There are reasonable safeguards against loss, misuse or disclosure; and
- If it is necessary to give information to another person, such as someone working on contract, everything reasonable is done to prevent unauthorised use or unauthorised disclosure of the information.

Principle 6 - Access to personal information

Where personal information is held in a way that it can readily be retrieved, the individual concerned is entitled to:

- Obtain confirmation of whether the information is held; and
- Have access to information about them.

An agency may refuse to disclose personal information for a range of reasons, including that it would:

- Pose risks to New Zealand's security or defence;
- Breach confidences with another government;
- Prevent detection of criminal offences or the right to a fair trial;
- Endanger the safety of an individual;
- Disclose a trade secret or unreasonably prejudice someone's commercial position;
- Involve an unwarranted breach of another individual's privacy;
- Breach confidence where the information has been gained solely for reasons to do with the individual's employment, or to decide whether to insure the individual;
- Be contrary to the interests of an individual under the age of 16;
- Breach legal professional privilege;
- Reveal the confidential source of information provided to a Radio New Zealand or Television New Zealand journalist; or
- Constitute contempt of court or the House of Representatives.

Requests can also be refused, for example, if the agency does not hold the information or if the request is frivolous or vexatious.

Principle 7 - Correction of personal information

Everyone is entitled to:

- Request correction of their personal information;
- Request that if it is not corrected, a statement is attached to the original information saying what correction was sought but not made.

If agencies have already passed on personal information that they then correct, they should inform the recipients about the correction.

Principle 8 - Accuracy of personal information to be checked before use

An agency must not use or disclose personal information without taking reasonable steps to check it is accurate, complete, relevant, up to date, and not misleading.

Principle 9 - Personal information not to be kept for longer than necessary

An agency holding personal information must not keep it for longer than needed for the purpose for which the agency collected it.

Principle 10 - Limits on use of personal information

Personal information obtained in connection with one purpose must not be used for another.

The exceptions include situations when the agency holding personal information believes on reasonable grounds that:

- The use is one of the purposes for which the information was collected; or
- The use is directly related to the purpose the information was obtained for; or
- The agency got the information from a publicly available publication; or
- The individual concerned has authorised the use; or
- The use is necessary for a public sector agency to collect the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or
- The use is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual; or
- The individual concerned is not identified; or
- The use is authorised by the Privacy Commissioner under section 54.

Principle 11 - Limits on disclosure of personal information

Personal information must not be disclosed unless the agency reasonably believes that:

- The disclosure is in connection with, or directly related to, one of the purposes for which it was obtained; or
- The agency got the information from a publicly available publication; or
- Disclosure is to the individual concerned; or
- Disclosure is authorised by the individual concerned; or
- It is necessary for a public sector agency to disclose the information to uphold or enforce the law, protect the tax base, or assist court or tribunal proceedings; or
- Disclosure is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual; or
- Disclosure is necessary to facilitate the sale of a business as a going concern; or
- The information is to be used in a form in which the individual concerned is not identified; or
- Disclosure has been authorised by the Privacy Commissioner under section 54.

Principle 12 - Unique identifiers

Unique identifiers - such as IRD numbers, bank customer numbers, driver/s licence and passport numbers - must not be assigned to individuals unless this is necessary for the organisation concerned to carry out its functions efficiently. The identifiers must be truly unique to each individual (except in some tax related circumstances), and the identity of individuals must be clearly established. No one is required to disclose their unique identifier unless it is for, or related to, one of the purposes for which the identifier was assigned.

The Government is not allowed to give people one personal number to use in all their dealings with government agencies.

Exceptions to the principles

Many of the principles have built-in exceptions. It's important to read the principles together with their exceptions to see how they relate to particular circumstances. The exceptions to principle 6 are set out in sections 27-29 of the Act.

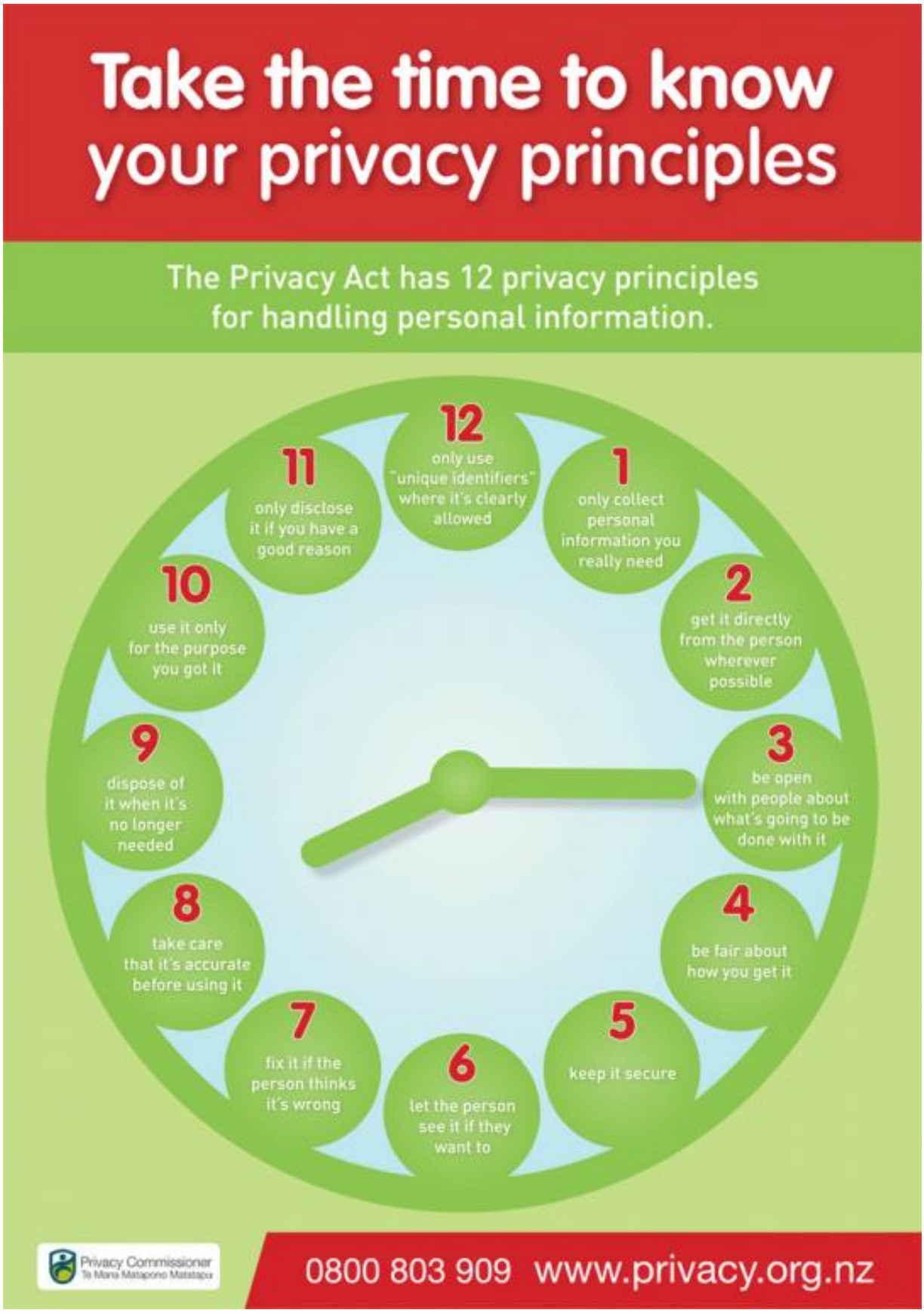
It's up to the person wanting to claim that an exception applies to prove that the exception applies.

Section 7 of the Privacy Act states, in effect, that if another statute is contrary to the privacy principles, that other statute will 'trump' the Privacy Act.

The privacy principles do not cover an individual who collects or holds personal information solely or principally for personal, family or household reasons.

This fact sheet is designed to provide general information about the Privacy Act 1993. It is not a detailed legal analysis. If you need more specific information, please see the Privacy Act in full, contact the Office of the Privacy Commissioner on 0800 803 909, email enquiries@privacy.org.nz or seek legal advice.

Privacy Principles Poster



Appendix 2: Sharing Information About Vulnerable Children

Sharing information about vulnerable children

Sharing information about an individual is often essential to their health, safety and wellbeing.

For social service agencies and their employees to do that job effectively, they often have to consult with each other to ensure that the right kind of intervention is made and at the right time. To do this, they need to share information while remaining on the right side of laws around personal, health and other information.

The Escalation Ladder

Sharing information involves both the collection and disclosure of personal information. Deciding which laws apply and what information to share can be complicated, but there are some guiding rules.

How to use the Escalation Ladder

Work through from question 1 to question 5 and stop when you can answer 'yes'. If the answer to all of the five questions is 'no', then disclosure should be unnecessary, and should be avoided, at least for now.

Remember that the proportionality principle always applies – you should only provide as much information as is reasonably necessary to achieve your objectives.

The escalation can be found at this link: https://privacy.org.nz/how-to-comply/sharing-information-about-vulnerable-children/

Appendix 3: ELI Privacy Information And Frequently Asked Questions

The Privacy Act 1993 aims to promote and protect individual privacy and requires careful treatment of all personal information, and this law applies to ELI. The Ministry of Education, together with the Office of the Privacy Commissioner, conducted a full Privacy Impact Assessment. Under sections 144A and 311(5) (a) of the Education Act 1989 the Ministry has the authority to collect information for the purposes of obtaining full, accurate and timely information about enrolment, attendance, and teaching at early childhood education (ECE) services.

In accordance with section 344 part 30 of the Education Act 1989 the Ministry will use the information collected in ELI for the purposes of:

- Monitoring and ensuring student attendance;
- Ensuring education providers and students receive appropriate resourcing;
- Statistical purposes;
- Research purposes;
- Ensuring student's educational records are accurately maintained.

This section of the Privacy Act 1993 prevents the National Student Number (NSN), or other numbers such as the National Health Index number, or tax number, becoming a single national number.

ELI stores all data securely with the In Confidence security classification to New Zealand government standards. ECE services are also responsible for ensuring that information collected about individuals is kept private in accordance with the Privacy Act 1993. This includes information like names, date of birth and addresses. Services should make sure that any copies of a child's official identification documents are kept in a secure location.

ECE services should limit the use of ELI Web or Student Management Systems (SMS) to authorised persons to submit accurate information to the Ministry, and to meet obligations for the careful treatment of personal information under the Privacy Act 1993.

Authorised users refer to:

- The ECE Service Provider Contact or delegated representative/s for the purpose of submitting data to the Ministry
- The Ministry data analyst or delegated representative for the purpose of educational research, statistics, monitoring, reporting to Government and the public, and resourcing.

Each parent can also request the information held about their child. There are no plans to share personal information with other Government departments.

Extensive security testing has been undertaken by the Ministry. All data is encrypted as it is sent across the internet. ELI Web requires services to use a logon and password as do SMSs. An ECE service can only access data related to their own service.

All activity on the National Student index is monitored and recorded by the Ministry. Authorised staff members must not search for students who are not enrolled in the service they are employed by. The Ministry's Code of Conduct states that misuse or disclosure of official information, which includes all personal information, could result in disciplinary action, including dismissal.

The Ministry strongly advises that services put in place appropriate processes to ensure that the privacy of information for enrolled children is maintained.

The Ministry also worked with the ECE Sector Advisory Group to develop the seven principles of ELI use which describe shared responsibilities, access to data, timeliness, ability to correct errors, and obligations of the Privacy Act 1993. You can download the Principles of ELI Use from the Resources page of this website from the All ECE Service**s** tab.

To find out more information about the Privacy Act and how to comply, go to: www.privacy.org.nz.

To read the Ministry of Education's **Privacy Impact Assessment** for ELI please see the document attached below.

ELI Information and Privacy – questions and answers

Common Terms

ECE	Early Childhood Education
NSN	National Student Number
SMS	Student Management System
Ministry	Ministry of Education

How frequently will data be sent to the Ministry?

This depends on the system your service is using to access ELI and your service's administration processes. ELI Web sends the data to the Ministry each night. Some SMSs will send the data daily, some weekly and some monthly.

What will the Ministry do with the information collected through the ELI?

The information collected in ELI will be used for the following purposes:

- Monitoring.
- Ensuring education providers and students receive appropriate resourcing.
- Statistical purposes.
- Research purposes.
- Ensuring that children's educational records are accurately maintained.

More generally the information will be used for educational research, monitoring, policy development, and funding. Other uses of ELI data will include:

- Regular statistics reporting.
- Inputs into forecasts on expenditure.
- Advice to Ministers.
- Reporting to Government, Parliament, and the public.
- Accounting for the numbers of children in ECE.

Who will have access to the information collected through the ELI?

Authorised users are able to access ELI and the information inputted for their respective service/s. Only the Ministry has access to all of the information collected by ELI.

What gives the Ministry the authority to collect this information?

The Ministry has the authority to collect this information under sections 144A and 311(5) (a) of the Education Act 1989. These sections of the Act give the Ministry the authority to collect information for the purposes of collecting full, accurate and timely information about enrolment, attendance and teaching/child contact at ECE services.

Does the Ministry have an information sharing agreements with any other parties?

No. The Ministry currently does not have any information sharing agreements with any other parties and has no plans to share detailed personal information with other Government departments.

Refer to the ELI Privacy Information page of the ELI Homepage for more information.

How will the Ministry protect children's privacy?

The Ministry has a number of measures in place to ensure the privacy of children. ELI sends data securely to the Ministry who have strict approval processes to restrict staff access to ELI data. The Ministry and all authorised users must comply with the obligations of the Privacy Act 1993.

What are ECE services' obligations to protect children's privacy?

- ECE services are responsible for ensuring that information collected about individuals is kept private. This includes information like names, dates of birth and addresses. All ECE services must comply with the Privacy Act 1993 which aims to promote and protect individual privacy and in particular to establish principles with respect to:
- the collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and
- access by each individual to information relating to that individual and held by public and private sector agencies.

More information can be found on the Privacy Information page and at www.privacy.org.nz.

How can we be sure the ELI is a secure system?

- Extensive security testing has been completed by the Ministry throughout the development of ELI. Access to ELI via ELI Web or an SMS requires authorised users to have a unique logon and password.

The Ministry has worked closely with the Office of the Privacy Commission to conduct a full privacy impact assessment