



Privacy Policy Noho Matatapu

Version 1 | Mahi Tuatahi
Effective Date | Whakamana tahito: June 2026 | Hune 2026
Next Review | ā houanga arotake: June 2028 | Hune 2028
Policy Owner | Rangatira Kaupapa Māhere: Chief Executive Officer
Key Accountabilities | Ngā Takonga Tuatahi: Chief Operating Officer

Introduction | Tīmatanga Kōrero

The purpose of this policy is to:

1. To acknowledge the information privacy principles contained in the Privacy Act 2020.
2. To ensure all He Whānau Manaaki o Tararua Free Kindergarten Association (Whānau Manaaki) members manage personal information in compliance with the Privacy Act 2020, other relevant laws, and the privacy promises made to all individuals concerned.

NB: The Privacy Act 2020 uses the term 'individual concerned' to describe any individual for whom personal information has been created, solicited, volunteered or otherwise relates to the organisations operations.

Background

3. Whānau Manaaki collects and processes personal information about our people, tamariki, parents and whānau, contractors, volunteers and other individuals and organisations that we are in relationship with. Every person who attends, works at or makes personal or professional contact with Whānau Manaaki is entitled to full privacy with regard to personal information, as specified in the Privacy Act 2020 ("the Act"). While Whānau Manaaki is required to comply with the Act, and its associated regulations, it also recognises the importance of this responsibility as a commitment to community and their expectations of Whānau Manaaki.
4. Privacy is particularly important for Kindergartens and Home-based services, which collect and process personal information about vulnerable people – including tamariki and their whānau – and may have to use or share personal information in ways that could impact on individual trust.
5. Whānau Manaaki recognises that individuals will only relinquish control of their personal information, or that of tamariki, if they trust us to use the information responsibly and treat it with care and respect. Whānau Manaaki has made a number of promises in its Privacy Statements and must be able to keep these promises. This policy seeks to ensure:
 - a. **Data minimisation** – limiting the amount of personal information Whānau Manaaki collects and holds
 - b. **Transparency** – being open and honest about what information Whānau Manaaki collects and how it will be used
 - c. **Security** – protecting the personal information Whānau Manaaki holds from harm.



- d. **Use limitation** – making sure Whānau Manaaki uses and discloses personal information only when necessary and with a lawful basis
- e. **Privacy rights** – helping Whānau Manaaki individuals concerned to exercise their privacy rights and maintain some control over their information.
- f. **Appropriate Management Protocols** – In addition to points a.- e. that in instances where errors, misrepresentation, mishandling, breaches or unwarranted retention occur, all individuals concerned may safely engage in culturally safe, corrective and restorative processes without further harm.

Applies To | Ko Wai Whakahāngaitia

6. This policy applies to all He Whānau Manaaki o Tararua Free Kindergarten Association employees, volunteers and contractors (Whānau Manaaki).

Definitions | Whakamāramatanga

7. The following definitions apply to this policy:

Individual Concerned

Any natural person about whom the Whānau Manaaki collects and holds personal information and includes tamariki, parents and whānau, staff members, contractors, any other persons listed in a child's enrolment and visitors to any Whānau Manaaki locations or online sites.

Lawful Purpose

A purpose that is directly connected with any of the lawful functions and operations of Whānau Manaaki, and includes, but is not limited to considering applications for employment or enrolment at a Whānau Manaaki service; administering professional learning and development; managing staff and ensuring the health and safety of tamariki and staff members; and meeting Whānau Manaaki reporting requirements.

Personal Information

Any information, whether electronic or hard copy, about an individual concerned, whether or not the information directly identifies the individual concerned, and includes but is not limited to contact, demographic, health records (including ACC), qualifications information, CCTV footage, staff performance information, emails and other correspondence, and opinions about the individual concerned. Examples of personal information include, but are not limited to:

- parent email addresses and phone numbers,
- child learning records,
- photos or videos of tamariki posted on social media,
- NHI numbers
- Personnel data



- Any other such detail that, on seeing or hearing it, would result in a person's identity being known.

Privacy Breach

An event (whether intentional or unintentional) in which personal information is lost or is accessed, altered, disclosed or destroyed without authorisation, or is at increased risk due to poor security safeguards, including but not limited to:

- a. accidental disclosure of personal information to the wrong recipient;
- b. employee browsing of personal information without a legitimate business reason;
- c. an external attack on a Whānau Manaaki system; or
- d. a lost or stolen Whānau Manaaki device or document.

Whānau Manaaki must notify the Privacy Commissioner and affected individuals if a breach is likely to cause serious harm. If such a notification is made, the Ministry of Education will also be advised and any actions required by either agency will be observed by Whānau Manaaki.

Privacy Framework

The collective body of information that governs Privacy for Whānau Manaaki. It includes this policy, and any procedures, standards or guidelines issued to support it.

Privacy Statement

A notice Whānau Manaaki has provided to a particular category of individuals concerned that outlines in general the matters set out at item 4 of this policy and includes the Privacy Statements specifically designed for parents and whānau, contractors, our people and for research purposes.

Whānau Manaaki Worker

Includes the Governance Board, staff members, volunteers, TONI Home Educators, and contractors working for and on behalf of Whānau Manaaki and, for the purposes of this Policy, includes any persons collecting or processing personal information in the course of research, or who are otherwise permitted access to personal information held by Whānau Manaaki.

General Principles | Mātāpono Whānui

Collection

8. Whānau Manaaki workers must collect, or must design a process or system to collect, only the personal information they need for a lawful purpose.
9. Where a process or system can operate without the collection of personal information, Whānau Manaaki will be permitted to use it anonymously.
10. Personal information should be collected from the individual concerned directly, unless an exception can be relied upon to collect it from a third party. Specifically, in the case of tamariki information, that the third party is legally authorised to act on the behalf of that tamariki (e.g., their parent or whānau member).

NB: Exceptions are listed in Information Privacy Principles (Principle 2) of the Privacy Act 2020. The usual basis on which we collect information from a third party is that:

- a. that non-compliance would not prejudice the interests of the individual concerned; and
- b. compliance is not reasonably practicable in the circumstances of the particular case.

11. At the time that personal information is being collected from an individual concerned, Whānau Manaaki workers must ensure that individual concerned are made aware:
 - a. what information is being collected
 - b. why the information is being collected
 - c. how the information will be used
 - d. who the information will be shared with, and
 - e. what rights they have to access and correct that information.
12. A full explanation of personal information, as it relates to tamariki, parents and whānau, including when and how consent for information sharing will be sought will be supplied when tamariki start with Whānau Manaaki.
13. If the information collected is a routine part of Whānau Manaaki process (that is, the collection of information is not unusual or is ad hoc), it will be sufficient for compliance with item 4 above if the worker refers or provides the individual concerned with a link to the relevant Privacy Statement. Occasional or ad hoc collections, such as surveys or research projects, will require the provision of specific privacy notices relating to that collection.
14. Where a new collection, use or disclosure of personal information is to become a routine part of Whānau Manaaki process, the responsible worker must ensure that the Privacy Officer is notified, and the relevant Privacy Statement is updated to reflect this.

Use and Disclosure

15. Except as provided in item 8, personal information must only be used or disclosed by Whānau Manaaki workers if that use or disclosure is the purpose for which it was collected and has been made clear to the individual concerned in the relevant Privacy Statement.
16. Before using or disclosing personal information in new ways, or in ways that are not part of the routine business of Whānau Manaaki, Whānau Manaaki workers must ensure that this is necessary for a lawful purpose or is otherwise permitted or required by law. Information sharing provisions are also included in other legislation that may be relevant, specifically:
 - the Oranga Tamariki Act 1989 and
 - the Family Violence Act 2018.
17. In addition, there are other legal statutes under which information must be disclosed, that relate to the maintenance of law and order. Specifically, the Search and Surveillance Act 2012, the Intelligence and Security Act 2017, or other statute containing search powers.

NB: Usually the best way to use or disclose information in new ways is to seek the authorisation of the individual concerned. If this is not practicable in the circumstances, Whānau Manaaki

members must be able to rely on an exception to Principle 10 (use) or Principle 11 (disclosure) of the Privacy Act 2020. If this is not clear, consult the Privacy Officer.

18. Whānau Manaaki workers must take reasonable steps to ensure that personal information is accurate and up to date before using or disclosing it, particularly where this use or disclosure could impact on the rights or interests of the individual concerned.
19. Whānau Manaaki will take an opt in approach to voluntary sharing of tamariki information, such as posting on social media or participation in televised events. This will involve appropriate event planning and obtaining informed consent before disclosing or using personal information, including images and video.
20. Before sharing personal information with a contracted service provider, or disclosing personal information to an overseas recipient (other than an individual concerned), Whānau Manaaki workers must ensure that the service provider or recipient is required and able to provide an adequate level of protection to the personal information shared. This would include ascertaining if there are comparable privacy laws, OR contractual safeguards, OR express informed authorisation.
21. In the event that a complaint is received under either the Complaints and Concerns Policy or the Protected Disclosures Policy, the complainant can expect that their concerns will be handled promptly, respectfully, and in accordance with our confidentiality obligations, with appropriate steps taken to investigate and respond in a manner that upholds the principles of this policy.
22. Individuals also have the statutory right to escalate any complaint of concern to the Privacy Commissioner, this can be supported with by sharing the relevant information for them to action themselves, or with us making a referral statement on their behalf.
23. Principles relating to Māori Data Sovereignty, tikanga and mana supporting narrative are critical considerations in use and disclosure decisions.

Access and Correction

24. Every individual concerned, or their authorised representative, has the right to request a copy of the personal information Whānau Manaaki holds about them, or to ask Whānau Manaaki to correct their personal information if they think it is wrong.

NB: For staff, volunteer and or contractors this should be completed via a case raised in the online HR management system Tūhonohono. For some changes the individual concerned should expect to complete a new Staff Information Form and/or a Proof of ID Form.

25. In kindergartens or home-based services, tamariki, parent or whānau information and other contacts, updates may be requested in writing or in person and actioned immediately by Whānau Manaaki workers.
26. Whānau Manaaki will respond to any access or correction requests within 20 working days. If that is not possible Whānau Manaaki will communicate with the requestor advising of the need for additional time, including an anticipated date for completion.

Security and Retention

27. All Whānau Manaaki workers have a responsibility to protect the personal information they handle against loss, misuse, or unauthorised access, modification or disclosure.
28. Information security is an important part of good personal information management. Whānau Manaaki workers must ensure that they have read and understood the relevant policies, having special regard to the File Management Policy, Complaints and Concerns Policy, and ICT and Cyber Safety Policy.
29. Whānau Manaaki workers must only access or use personal information – whether within an information system or in hard copy – when this is necessary for a legitimate business purpose. Unauthorised access or improper use will be considered misconduct and handled in accordance with the Disciplinary and Misconduct Policy.
30. Whānau Manaaki workers must not retain personal information for longer than the organisation has a lawful purpose to use it and must delete information in compliance with the Whānau Manaaki Retention and Destruction Policy. Minimum retention requirements must comply with the Public Records Act 2005 and any recording keeping requirements detailed in ECE related regulations.
31. Whānau Manaaki workers must ensure that any privacy breach they become aware of is reported promptly to the Privacy Officer in compliance with the Privacy Breach Management Procedures.

Responsibilities and Governance

32. All Whānau Manaaki workers must:
 - a. understand and comply with the Privacy Framework
 - b. actively participate in any privacy training provided by Whānau Manaaki, and
 - c. keep their Senior Leader, Senior Teacher, Team Leader and/or the Privacy Officer informed of any personal information requests, privacy issues or privacy breaches.
33. Senior Leaders, Senior Teachers, Team Leaders must:
 - a. support staff to understand and comply with this policy and participate in any privacy training provided by Whānau Manaaki, and
 - b. ensure personal information requests, privacy breaches and other privacy issues are identified and managed in accordance with the Privacy Framework.
 - c. ensure that culturally appropriate practices are embraced and applied, and are considered carefully in use, disclosure, access, retention, security and breach management decisions.
34. The Privacy Officer is responsible for:
 - a. supporting all Whānau Manaaki workers to understand and comply with the Privacy Framework, including by maintaining and developing relevant procedures, standards and guidelines
 - b. maintaining oversight of trends, risk management and privacy culture in consultation with the Privacy Working Group and other relevant senior leaders.

- c. assisting with the management privacy breaches and other privacy issues by Whānau Manaaki workers
- d. managing privacy complaints from individuals concerned
- e. reporting on privacy breaches and general privacy compliance to the Chief Executive Officer, and
- f. liaising with third parties in respect of privacy matters, including the Privacy Commissioner or other relevant regulators and individuals concerned.
- g. provision of appropriate monitoring and reporting of privacy related matters to the Senior Leadership Team and Governance Board.

35. The Privacy Officer can be contacted directly at privacy@wmkindergartens.org.nz

Relevant Legislation and Regulations | Whaitake Ture me Waeture

[Privacy Act 2020](#)

[Health Information Privacy Code 2020](#)

[Public Records Act 2005](#)

[Licensing criteria for ECE services – Education in New Zealand](#)

[Oranga Tamariki Act 1989](#)

[Family Violence Act 2018](#)

[Protected Disclosures \(Protection of Whistleblowers\) Act 2022](#)

Related Procedures or Processes and Documents | Pākanga Tukanga me Pukapuka

Privacy Statements (Our People, Piri'anga Alofa clients, and Parents and Whānau)

Privacy Breach Management Procedures

Privacy Procedures (Breach Management, Kindergarten, Our People, Etu Ao)

Enrolment and Admission, Induction and Parent & Whānau Engagement Policy

File Management Policy

Complaints and Concerns Policy

Digital and Cyber Safety Policy

Disciplinary and Misconduct Policy

Protected Disclosures Policy

Media Consent Forms

Policy Review Cycle | Kaupapa Arotake Hurihanga

This policy is to be reviewed every two years. Whānau Manaaki may amend or cancel this policy or introduce a new policy, as it considers it necessary within the current cycle of the policy. Any amendments will be considered by the policy Working Group and will need to be approved by the Senior Leadership Team and the Board. The policy will continue on the same review cycle.



Breach Management | Whakahaere Takahi Tūmataiti

Version 3 | Mahi Tuatoru

Effective Date | Whakamana tahito: June 2026 | Hune 2023

Next Review | ā houanga arotake: June 2026 | Hune 2026

Policy Owner | Rangatira Kaupapa Māhere: Chief Executive Officer Key
Accountabilities | Ngā Takonga Tuatahi: Chief Operating Officer

Application | Ko Wai Whakahāngaitia

These procedures apply to all Whānau Manaaki staff members, contractors, and to any volunteers working at Whānau Manaaki.

Introduction | Tīmatanga Kōrero

Purpose

To ensure that privacy breaches are managed in accordance with the Whānau Manaaki Privacy Policy and in compliance with our obligations under the Privacy Act 2020, including privacy breach notification requirements.

Introduction

Whānau Manaaki's Privacy Framework includes a high-level Privacy Policy, privacy procedures, and a set of Privacy Statements. All Whānau Manaaki workers are expected to manage personal information in accordance with Whānau Manaaki's Privacy Framework.

These procedures – and New Zealand's breach notification regime – are intended to ensure transparency and accountability, not blame. All Whānau Manaaki workers and our communities should feel safe to speak up and have confidence that concerns will be handled in a manner that is culturally appropriate, respectful and can be learnt from. Once alerted to a privacy breach, Whānau Manaaki can take steps to manage it. The procedure requires speed, care and collaboration. It is important to include the right people, at the right time, in the right ways.

A privacy breach in relation to personal information held by Whānau Manaaki could cause harm to our people, tamariki, parents and whānau or other individuals. A privacy breach could also, if managed badly, significantly damage the reputation of Whānau Manaaki. When there is a likelihood that a privacy breach could cause serious harm, Whānau Manaaki is required to notify the Privacy Commissioner and the individuals affected. This is called a notifiable privacy breach.

Procedures | Nga Tikanga

Report

1. Any member of the wider Whānau Manaaki community who causes or discovers a privacy breach must as soon as practicable report the breach to their Team Leader, Head Teacher, Senior Teacher, Senior Leader and/or the Privacy Officer. In the event that a report is made to someone other than the Privacy Officer, then they must be notified also, at the earliest opportunity.
2. Where the privacy breach is also an IT security incident, the breach must also be reported to the Digital Operations Manager who will initiate an investigation.
3. Where the privacy breach is not also an IT security incident, the Privacy Officer must report the privacy breach to SLT within 24 hours of becoming aware of the breach.





4. On notice of a breach, the Privacy Officer (or delegated authority) will immediately initiate an investigation and create a secure folder for the deposition of all relevant documentation. Responsibility for the investigation and associated reporting sits with the Privacy Officer, or their delegated authority. The finalised investigation will record decision-making rationale, key findings and next steps.
5. Notwithstanding any other provision made within these procedures, any member of the wider Whānau Manaaki community who recognises that a privacy breach was narrowly avoided, may elect to report the near miss to their Team Leader, Senior Teacher, Senior Leader and/or the Privacy Officer for the purpose of contributing to the emergent review of either service level procedures and/or organisational policy.

Contain and Assess

6. The Privacy Officer must, on receipt of a report and in liaison with the relevant leader(s), determine the scope of the privacy breach, including the types of data and individuals affected, the sensitivity of the personal information at risk, and evaluate the likelihood of harm to the individuals affected.
7. The relevant leader must, under the guidance of the Privacy Officer and/or the CEO, determine what steps, if any, are required to contain the privacy breach, including steps that the individuals affected might take.
8. Additional guidance and considerations for containing, assessing, notifying and prevention are detailed in [Appendix A](#).

Notify (Privacy Officer)

9. The Privacy Officer must determine whether the privacy breach is a notifiable privacy breach.

Note: Factors that may be relevant to this determination include the sensitivity of the personal information involved, nature of the harm that may be caused, whether the information was protected by security measures, the distribution of the information and the nature of the recipient, and the ability to contain the breach or its consequences. It should also be noted that the test for emotional harm is subjective, and so consideration should be given to the particular sensitivities of the individual(s) affected.

Assessment of harm may mean contacting the individual or family affected. Especially in instances where it is unlikely Whānau Manaaki staff are aware all the relevant details that could result in harm in a whānau context, for example, family court proceedings, stalkers etc.

10. Where the Privacy Officer has determined that the privacy breach is a notifiable privacy breach, the Privacy Officer must prepare notifications to the Privacy Commissioner, or any other relevant regulator, and the individual(s) affected.
11. Privacy breach notifications must be made to the Privacy Commissioner and individuals affected as soon as practicable after Whānau Manaaki has become aware of the privacy breach.





12. Notification to the Privacy Commissioner may only be made by the Privacy Officer, Senior Leader or Chief Executive Officer.
13. The Privacy Officer may, where appropriate, direct the relevant leader or another employee to manage the notification of the individuals affected.

Prevent

14. The senior leader of the relevant work group will initiate an investigation into the reasons for the breach. This investigation may be completed by relevant employees, as the Privacy Officer and Chief Executive Officer consider appropriate.
15. If the privacy breach is also an IT security incident, the investigation must be conducted in conjunction with the Digital Operations Manager. Any findings must be reported to the Chief Executive Officer and the Privacy Officer.
16. Having considered the findings the Chief Executive Officer will determine what, if any, action is to be taken.

Definitions

IT security incident

attempted or successful unauthorised access, use, disclosure, modification or destruction of information, interference with IT operations, impersonation of any member of the Whānau Manaaki community through electronic and/ or social media, spoofing, or setting up any web presence (including presence on social media) that purports to be, or might reasonably be perceived to be, an official Whānau Manaaki website or social media group, page or account.

Notifiable privacy breach

A privacy breach that it is reasonable to believe has caused, or is likely to cause, serious harm to an individual or individuals.

Personal information

Any information, whether electronic or hard copy, about an individual concerned, whether or not the information directly identifies the individual concerned, and includes but is not limited to contact, demographic, health and academic information (including course results), CCTV footage, staff performance information, emails and other correspondence, and opinions about the individual concerned. Examples of personal information include, but are not limited to:

- parent email addresses and phone numbers,
- child learning records,
- photos or videos of tamariki posted on social media,
- NHI numbers
- Personnel data
- Any other such detail that, on seeing or hearing it, would result in a person's identity being known.





Privacy breach

An event (whether intentional or unintentional) in which personal information is lost or is accessed, used altered, disclosed or destroyed without authorisation, or is at increased risk due to poor security safeguards, including but not limited to:

- an IT security incident that relates to personal information;
- accidental disclosure of personal information to the wrong recipient;
- employee browsing of personal information without a legitimate business reason; or
- a lost or stolen Whānau Manaaki device or document.

Serious harm

Serious harm is assessed in accordance with sections [69\(2\)\(b\)](#) and [113 of the Privacy Act 2020](#). Further advice on whether an incident reaches the threshold for serious harm can also be sought from the Office of the Privacy Commissioner.

Appendix A – Guidance and Considerations for Breaches

Contain

Once you discover a privacy breach has occurred, you should act immediately to contain it. Steps to help contain a breach could include:

- Diagnosing what went wrong and disabling any systems that may be compromised until they have been secured.
- If we can remotely wipe information from devices that was mistakenly sent to someone by you, we should do so.
- Trying to retrieve lost information, e.g. if you have sent a letter to the wrong person, see if you can get the recipient to send it back unopened.
- Cancelling or changing computer access codes and fixing any weaknesses in the organisation's physical or electronic security.
- Appointing someone within the organisation to lead and conduct an initial investigation into what has happened. A more detailed review can be carried out later if necessary.
- Assembling a response team. Such a team may include people from within the organisation as well as external parties which have the expertise to deal with the situation.
- Considering who outside the organisation needs to be told about the breach, such as NetSafe - also, assessing whether your insurer, internal auditors, risk managers and legal advisers need to be informed.

Extra Tips

- If the breach involves theft or other criminal activity, inform the Police.
- Do not destroy information. It may be needed by your organisation or Police to find the cause of the issue.

Assess

Assessing a privacy breach as quickly as possible can help us understand the steps needed to appropriately respond.





Knowing what information is involved will help determine whether serious harm has occurred or is likely to occur and whether it is appropriate to tell the individuals affected.

The criteria for assessing the likelihood of serious harm stemming from a privacy breach is laid out in [section 113 of Privacy Act 2020](#). Those criteria are:

- **Any action taken by the organisation to reduce the risk of harm following the breach**
Have you taken steps to contain the breach? See *Contain* above.

Try to identify the size and scope of the breach, including the number and nature of the likely recipients as well as the number of affected people. Identify the risk of the information being circulated further and respond accordingly.
- **Whether the personal information is sensitive in nature**
The more sensitive the information involved in a breach, the higher the risk of harm to the people affected. Sensitive information is typically personal information relating to someone's health, genetic or ethnic background, finances, identity documents, political or religious beliefs, sex life or sexual orientation.

Sensitive information may also relate to whether someone is affiliated with a trade union or if they have committed any crimes. The disclosure of a person's sensitive information may cause them serious harm.

Context matters. Personal information which might not normally be considered sensitive, such as email addresses, may, in specific circumstances, be considered sensitive.
- **The person or body that has obtained or may obtain personal information because of the breach (if known)**
Was the receiver a trusted, known person or organisation that can be expected to return the information?

Or, was the information taken by, or given to, an unknown receiver, someone who might pose a particular risk, or to a wide range of people who may include those who might misuse the information?

Knowing who has received the information to inform the response.
- **Whether the personal information is protected by a security measure**
If breached personal information is password secured or encrypted, there is a lesser chance of it being accessed and misused than if it is unprotected.

You should consider whether the security measures that protect information involved in a breach are likely to be effective at preventing access to it in the circumstances?
- **Any other relevant matters**

Notify

Being open and transparent with people about how personal information is being handled is a fundamental rule of privacy, especially when there has been a breach. Notification can also be a key step in helping people affected by a breach.





If a privacy breach creates a risk of serious harm to people, those affected should generally be notified. Prompt notification can enable people to take steps to protect themselves and regain control of their information.

When should you notify people?

We must inform the Privacy Commissioner of serious privacy breaches as soon as practical after becoming aware of them, without undue delay. We can do this using [NotifyUs](#). If a breach looks serious at the discovery stage, report it rather than taking a 'wait and see' approach.

In most cases, we will also need to notify the people affected by the breaches unless an exception applies, such as if notifying them would adversely affect that person's mental health.

Only notify people if you are sure their information has been compromised by the breach and that you know that the breach is likely to cause serious harm.

Incorrectly notifying the wrong people that their information has been breached may cause them unnecessary stress and harm.

If there is no risk of serious harm, it is not necessary to notify people of a privacy breach. Sometimes, notification can do more harm than good. Each incident needs to be considered on a case-by-case basis.

Things to consider:

- What is the risk of harm to people whose information has been breached?
- Is there a risk of identity theft or fraud?
- Is there a risk of physical harm?
- Is there a risk of humiliation or loss of dignity, damage to someone's reputation or relationships? For example, when the lost information includes mental health, medical or disciplinary records?
- What is the person's ability to avoid or minimise possible harm?
- What are the legal and contractual obligations?
- Consider the impact notification of a breach may have on at-risk people. You may then decide not to inform them or do so with particular care.

The [NotifyUs](#) tools should be used to assess how serious your breach is and whether you will need to notify the Privacy Commissioner.

If law enforcement authorities are involved, check with those authorities on when to notify so that their investigation is not compromised.

You don't always need to notify the people involved, or give public notice, of a notifiable privacy breach.

When you don't need to notify

There is no requirement to notify the people involved, or give public notice, of the notifiable privacy breach if you believe that the notification or public notice will:

- prejudice the security, defence, or international relations of New Zealand
- prejudice the maintenance of the law by a public sector agency
- endanger someone's safety, or
- reveal a trade secret.





Notifying someone else – at-risk people

While there is no requirement to notify a person about, or give public notice of, a notifiable privacy breach involving their personal information if the person is under the age of 16, we must notify the person's parent, guardian or other representative (rather than notify the person involved or give public notice) if they are a child enrolled in a Whānau Manaaki service.

Delaying notification or public notice

We can also delay notifying the people involved, or giving public notice, of the notifiable privacy breach if we believe that:

- the notification or public notice may have risks for the security of personal information that we hold for example, if we have to patch a security exploit to avoid a further privacy breach); and
- those risks outweigh the benefits of informing the affected people.

However, we can delay the notification or public notice only while those risks continue to outweigh those benefits.

In any case, we should not delay or refuse to contact the Privacy Commissioner about a notifiable privacy breach.

How to notify affected people

It is always best to notify affected people directly - by phone, letter, email or in person. Direct notification is more sincere and personal.

Who should notify people?

We have direct relationships with our people as well as parents and whānau, consequently we should be the people to notify the affected people.

What to say?

Breach notifications to individuals should generally include:

- Information about the incident, including when it happened.
- A description of the personal information that was disclosed and what has not been disclosed.
- What the organisation is doing to control or reduce the harm.
- What the organisation is doing to help people and what steps those affected can take to protect themselves.
- Contact information for enquiries and complaints.
- Offers of assistance when necessary, for example, advice on changing passwords.
- Whether the organisation has notified the Office of the Privacy Commissioner.
- Contact information for the Privacy Commissioner.

Notifying third parties

Organisations should consider whether the following groups or organisations should also be informed.

Bear in mind any obligations of confidentiality.

- Police
- insurers





- professional or other regulatory bodies
- credit card companies, financial institutions or credit reporting agencies
- third party contractors or other parties who may be affected
- internal business units not previously advised of the privacy breach, for example, government relations, communications and media relations
- other members of senior management
- the board
- the government minister
- union or other employee representatives.

Prevent

There are several steps Whānau Manaaki will take to minimise or prevent future privacy breaches.

In all instances we will undertake a review of our procedures and practices with a view to improvement.

We will have, or develop where necessary, well thought out ICT security, event management and consent plans for all personal information we hold.

We will review policies with a view to minimise the collection and retention of personal information, investigate the cause of any breaches experienced and update our prevention plans.

The significance of a breach, and whether it happened due to a systemic problem or an isolated event, will be a key consideration in informing the steps needed to prevent future breaches.

These steps could include:

- an audit of both physical and technical security
- a review of policies and procedures
- a review of employee training practices
- a review of contributing actions and behaviours
- a review of any service delivery partners caught up in the breach.

It is important that teams regularly review their procedures and/or undertake privacy refreshers to ensure the policy and expected actions are well known.





This privacy statement explains how Whānau Manaaki collect and manage the personal information we hold about people employed, studying with us or in formalised volunteering roles. It outlines the types of personal information we collect, how we use and share it, and the rights you have to access or correct personal information we hold.

Whānau Manaaki recognises that you will only share your personal information, or that of whānau members, if you trust us to use the information responsibly and treat it with care and respect.

Types of personal information we collect or create

We need to collect a wide range of personal information from our people in order to deliver early childhood education services and to ensure the safe and appropriate management of our people resources.

The types of personal information that we collect depends on the circumstances of collection and the relationship with the individual the information is about.

You do not have to provide us with all the personal information we request. However, at employment, most of what is collected is required either by the Ministry of Education (regulations and licensing criteria) or under the stipulations of the Employment Relations Act 2000. Other personal information is created through the course of your employment and/or your relationship with us.

We will always explain when personal information is really needed and can discuss any concerns you may have about providing it to us. The following personal information may be collected or created:

- Full name
- Contact details and emergency contacts
- Date of birth
- Gender, ethnicity and other demographic information
- Qualifications, certifications, registrations or other professional body memberships
- Employment history
- Financial information, including payroll, payment/reimbursement details and allowances
- Health information where this is relevant to the safe delivery of early childhood education services, such as immunisations, health conditions or other risks
- Protection orders, restraining orders, or other legal stipulations that may impact the safety of tamariki or other staff
- Justice and/or Corrections histories, including criminal history or any activities likely to impact safety checking outcomes
- Actual and perceived conflicts of interest
- Photographs, audio, video or other media (for example during kindergarten activities or a special events)
- Notes taken by staff, including relating to any incidents relating to tamariki, investigations or, complaints and concerns
- Information relating to your whānau circumstances (e.g. intended parental leave arrangements)
- Correspondence or recorded communications with our Parents and Whānau, Kindergarten staff or volunteers

How we use and disclose personal information

Our primary purpose for collecting personal information is to safely deliver early childhood education services and to ensure the appropriate management of our people resources. To do this, we need to use, and sometimes share, personal information in the ways set out below. If we need to use or share personal information in a way we have not anticipated here, we will only do so if required or permitted by law, and/or with your consent.

We use personal information to:

- Provide early childhood education services to our tamariki and their whānau.
- Ensure the educational, social and medical wellbeing of our tamariki and our staff.
- Ensure the safety and health of our tamariki, staff, students, volunteers, contractors and visitors.
- Manage and administer our kindergartens.
- Meet legislative and regulatory requirements, including the requirements of the Children's Act 2014, the Education and Training Act 2020, the Employment Relations Act 2000, the Health and Safety Act 2015, the ECE Regulations 2008 and the Licensing Criteria
- Inform activities to support the achievement of our strategic intentions, contracts, agreements and, other obligations.

Disclosure

We may need to disclose personal information to third parties in order to meet the purposes set out above, including to:

- Education Review Office, where necessary to meet reporting or audit requirements.
- New Zealand Police, where Police Vetting is required, or it is necessary to keep tamariki safe from harm.
- Oranga Tamariki, where we believe you or tamariki may be at risk of harm.
- Te Whatu Ora | Ministry of Health and National Public Health Service, where directed or required to ensure the health of tamariki. Te Whata Ora | Ministry of Health and National Public Health Service store information securely and treat it in accordance with both the Health Information Privacy Code 2020 and the Health Act 1956.
- Ministry of Social Development, where directed or required to provide assurance relating to accreditation or contract obligations.
- Ministry of Education, where directed to as stipulated below, to satisfy our legislative, regulatory and licensing obligations.
- Unions (NZEI Te Riu Roa) or Professional Bodies (e.g. Teaching Council), in the course of collective employment negotiations or as part of any mandatory reporting process.

Information is disclosed to the Ministry of Education as required:

- for funding allocation purposes
- for monitoring purposes
- for investigations (Health and Safety, complaints, Child Protection) and notifiable events (notifications to Police, Oranga Tamariki, the Privacy Commissioner or WorkSafe)
- to allow the Minister or Secretary of Education to exercise any of their other powers or responsibilities under the Education and Training Act 2020, and as permitted by Privacy Principles 10 and 11.

Completed forms may also be viewed by Ministry officials on request for the purposes of monitoring, regulatory compliance and licensing.

Photographs and recordings

Our staff, students and volunteers may use kindergarten devices to take photographs, or record video or audio footage of kindergarten activities. We do this primarily to keep parents and whānau updated on the activities their tamariki have been involved in while they are with us. However, it is not unusual for our people to also be included. Where these have already been shared with consent, we may also use photographs in our social media accounts, marketing materials or organisational documents. If we intend to use an image of you in collateral that will be publicly available (e.g., Annual Report or advertising posters) we will seek specific consent to do so.

How we store and protect personal information

We store personal information electronically (on secure systems or platforms, including cloud platforms) or in hardcopy (in a secure physical location, including lockable cabinets). We may use third-party service providers to store and process personal information for us, some of which may store or process information overseas. Information is only stored overseas when Whānau Manaaki is satisfied that appropriate safeguards exist, either within contractual guarantees or comparable legislative protections.

We retain personal information only for as long as we have a lawful purpose to use it, and we securely destroy the information we no longer need.

We take all reasonable steps to protect personal information from loss, misuse, or unauthorised access or disclosure. You can find more information about the Whānau Manaaki Privacy Framework in [Te Kete Mātauranga](#).

Whānau Manaaki expects that all reasonable steps are taken at both office and service (kindergarten, homebased, contract) level to ensure that these standards are maintained and expectations met, at all times.

Anonymous Protected Disclosure

In the event of a complaint made by Whānau Manaaki kaimahi | employees, volunteers, contractors, and Board Members, in accordance with the Protected Disclosures Police, you may make that complaint anonymously. However, an anonymous disclosure may make it difficult for Whānau Manaaki to properly investigate the matters disclosed if a report is submitted anonymously.

Therefore, disclosers are encouraged to share their identity when making a disclosure, although they are not required to do so. If a discloser shares their identity, Whānau Manaaki will use its best endeavours to keep confidential any information that might identify the discloser.

Where a disclosure has been made externally and you provide your contact details, those contact details will only be provided to an internal Receiver with your consent or otherwise where this is allowed in accordance with our Protected Disclosures Policy.

Accessing or correcting personal information

All of our people (employees, students, volunteers) will have the right to request a copy of the personal information we hold about them, or to correct their information if they believe it is wrong.

You can request a copy of the personal information we hold on you by contacting the [People Team](#) and/or the [Privacy Officer](#). You will be expected to verify your identity to ensure that information is shared only with the person to whom it relates. This may include being asked a series of questions based on your personnel record, or by providing photo identification (i.e. Driver's Licence or Passport).

All requests for personal information will be responded to within 20 working days. However, depending on the volume of information or the manner in which it has been retained, some information may take longer to compile than expected. If this occurs you will be contacted to discuss a revised timeline.

If you are not satisfied with the response you have received, you can lodge a complaint or contact the office of the Privacy Commissioner (www.privacy.org.nz).



Privacy Statement for Parents and Whānau Te Whakapumautanga Matatapu mo Matua me Whānau

Version 3 | Mahi Tuatoru

This privacy statement explains how Whānau Manaaki manage the personal information we hold about tamariki and their parents or whānau. It outlines the types of personal information we collect, how we use and share it, and the rights parents and whānau named on a tamaiti enrolment forms have to access or correct personal information we hold on you, or your tamaiti.

Whānau Manaaki recognises that you will only share your personal information, or that of tamariki, if you trust us to use the information responsibly and treat it with care and respect.

Types of personal information we collect or create

We need to collect a wide range of personal information about tamariki and their parents or whānau in order to deliver early childhood education services. The types of personal information that we collect depends on the circumstances of collection and the relationship with the individual the information is about.

You do not have to provide us with all the personal information we request. However, at enrolment, most of what is collected is required by the Ministry of Education. We will always explain when personal information is really needed and can discuss any concerns you may have about providing it to us.

We may collect or create the following personal information.

Information	Tamaiti	Parent or Guardian
Full name	Yes	Yes
Contact details and emergency contacts	Yes	Yes
Date of birth	Yes	No
Gender, ethnicity and other demographic information	Yes	No
Health information where this is relevant to the delivery of early childhood education services, such as immunisations, prescriptions, health conditions or other risks	Yes	No
Protection orders, custody agreements, or other legal documents relevant to the tamaiti	Yes	Yes
Photographs, audio, video or other media (for example during kindergarten activities or a special events)	Yes	No
Notes taken by staff, including relating to any incidents relating to the tamaiti (for example accidents or incidents involving a child during kindergarten activities)	Yes	Yes
Information about children's welfare, including whānau circumstances	Yes	Yes
Financial information, including invoices, payment details and payment history	No	Yes
Correspondence with our Kindergarten staff or volunteers	Yes	Yes
To allow the assignment of a National Student Number* to your child	Yes	No
* A national student number (NSN) is a unique education number which is allocated to children when they first enrol in ECE. Information about each child's attendance in ECE will be recorded against the NSN. The NSN stays with the child throughout their education, into the compulsory and tertiary sectors. It is a mandatory requirement of Schedule 24 of the Education and Training Act 2020 to assign NSNs to all children enrolled in early learning services in New Zealand		



He Whānau Manaaki o Tararua
Free Kindergarten Association Incorporated

Unit F, 15 John Seddon Drive, Elsdon, Porirua | PO BOX 50-743, Porirua, 5240
Telephone: 04 232 3069
Website: wmkindergartens.org.nz

How we use and disclose personal information

Our primary purpose for collecting personal information is to deliver early childhood education services. To do this, we need to use, and sometimes share, personal information in the ways set out below. If we need to use or share personal information in a way we have not anticipated here, we will only do so if required or permitted by law, or with your consent. All information relating to tamariki is considered highly sensitive.

We use personal information to:

- Provide early childhood education services to our tamariki and their whānau.
- Ensure the educational, social and medical wellbeing of our tamariki.
- Ensure the safety and health of our tamariki, staff, students, volunteers, contractors and visitors.
- Manage and administer our kindergartens.
- Communicate with our parents/guardians about their tamariki or more generally to provide information about events or important notices.
- Meet legislative and regulatory requirements, including the requirements of the Children's Act 2014, the Education and Training Act 2020, the ECE Regulations 2008 and the Licensing Criteria
- Inform activities to support the achievement of our strategic intentions, marketing activities and communications.

We may need to disclose personal information to third parties in order to meet the purposes set out above, including to:

- Volunteers and students working at a kindergarten, where necessary for them to undertake their duties. (i.e. Police Vetting)
- Education Review Office, where necessary to meet reporting or audit requirements.
- New Zealand Police, where necessary to keep tamariki safe from harm.
- Oranga Tamariki, where we believe a tamaiti may be at risk of harm.
- Te Whatu Ora and National Public Health Service, where directed or required to ensure the health of tamariki. Te Whata Ora and National Public Health Service store information securely and treat it in accordance with both the Health Information Privacy Code 2020 and the Health Act 1956.
- Ministry of Education; Personal information about your child is shared with the Ministry of Education who store it securely and treat it in accordance with the Privacy Act 2020.

Information is disclosed to the Ministry:

- for funding allocation purposes
- for monitoring purposes
- to allow the assignment of a National Student Number to your child, and
- to allow the Minister or Secretary of Education to exercise any of their other powers or responsibilities under the Education and Training Act 2020, and as permitted by Privacy Principles 10 and 11.

Completed forms may also be viewed by Ministry officials on request for the purposes of monitoring, regulatory compliance and licensing.

A note about the use of photographs

Our staff, students and volunteers may use kindergarten devices to take photographs of, or record video or audio footage of, tamariki. We do this primarily to keep parents and whānau updated on the activities their tamariki have been involved in while they are with us. With parent and whānau consent, we may also share photographs with through StoryPark or Facebook, or use photographs in our social media accounts, marketing materials or organisational documents (e.g., Annual Report or Strategic Plan).

Parent and whānau consent is obtained at enrolment for Facebook. Consents for sharing group stories are also obtained at enrolment, but all other applicable privacy conditions are to Storypark are governed through the application itself.

If we intend to use an image of your tamaiti in collateral that will be publicly available (e.g., Annual Report or advertising posters) we will seek specific consent to do so.

How we store and protect personal information

We store personal information electronically (on secure systems or platforms, including cloud platforms) or in hardcopy (in a secure physical location, including lockable cabinets). We may use third-party service providers to store and process personal information for us, some of which may store or process information overseas. Information is only stored overseas when Whānau Manaaki is satisfied that appropriate safeguards exist, either within contractual guarantees or comparable legislative protections.

We retain personal information only for as long as we have a lawful purpose to use it, and we securely destroy or de-identify the information we no longer need.

We take all reasonable steps to protect personal information from loss, misuse, or unauthorised access or disclosure. You can find more information about the Whānau Manaaki Privacy Framework [here](#).

Accessing or correcting personal information

All people we deal with have the right to request a copy of the personal information we hold about them, or to correct their information if they believe it is wrong.

In practice, parents and whānau can generally request a copy of the personal information we hold about their tamaiti, on the basis that they are acting as a representative for their tamaiti. However, we will always act in the best interests of tamariki, and if we believe that releasing personal information about tamariki to a parent or whānau member may not be in their best interests, we may refuse.

In the first instance, please send access or correction requests, or any complaints or concerns about privacy, to your Head Teacher. If they cannot assist, they will escalate the request or concern to their Senior Teacher, or another Senior Leader, or to the Whānau Manaaki Privacy Officer.

You will be expected to verify your identity to ensure that information is shared only with the person to whom it relates. This may include being asked a series of questions based on information you have already supplied, and/or by providing photo identification (i.e. Driver's Licence or Passport).

All requests for personal information will be responded to within 20 working days. However, depending on the volume of information or the manner in which it has been retained, some information may take longer to compile than expected. If this occurs you will be contacted to discuss a revised timeline.

If you are not satisfied with the response you have received, you can lodge a complaint with Whānau Manaaki or contact the office of the Privacy Commissioner (www.privacy.org.nz).



Kindergarten Privacy Procedures | Nga Tikanga Matatapu

Version 1 | Mahi Tuatahi

Effective Date | Whakamana tahito : June 2026 | Hune 2026

Next Review | ā houanga arotake: June 2028 | Hune 2028

Policy Owner | Rangatira Kaupapa Māhere: Chief Executive Officer

Key Accountabilities | Ngā Takonga Tuatahi: Chief Operating Officer

Application | Ko Wai Whakahāngaitia

These procedures apply to all Whānau Manaaki Members who work for or with Whānau Manaaki's Kindergartens, and to any volunteers, including whānau.

Introduction | Tīmatanga Kōrero

Purpose

These procedures support the Whānau Manaaki Privacy Framework, outlining specific privacy procedures and considerations relating to the management of personal information by Whānau Manaaki's Kindergartens.

Background

Whānau Manaaki's Privacy Framework includes a high-level Privacy Policy, privacy procedures relating to Disclosure, and Privacy Breach Management, and a set of Privacy Statements. All Whānau Manaaki members are expected to manage personal information in accordance with Whānau Manaaki's Privacy Framework.

Privacy is particularly important for Kindergartens, which collect and process personal information about vulnerable people – including tamariki and their whānau – and may have to use or share personal information in ways that could impact on individual trust. These procedures are intended to help Kindergartens to manage their specific regulatory and safety requirements in a way that protects and respects tamariki and whānau privacy.

Procedures | Nga Tikanga

Kindergartens must generally manage personal information in accordance with Whānau Manaaki's Privacy Policy and associated procedures, with the exception of the specific procedures set out below. In the event of any inconsistency between these procedures and Whānau Manaaki's general Privacy Policy and associated procedures, the procedures will prevail.

Governance

1. Each Senior Head Teacher (SHT) or Head Teacher (HT) will act as the first line Privacy Officer for their specific kindergarten. The Senior Teacher (ST) Team will provide support, and a point of escalation, to SHTs and HTs where required. The STs will escalate significant privacy issues to Whānau Manaaki Privacy Officer (Chief Operating Officer) where required. If necessary additional advice will be sought by the Associations legal counsel.

Collection

2. Kindergartens must collect only the personal information they need to deliver services and meet their regulatory and other requirements. The types of personal information we collect about tamariki and their whānau are listed in the Privacy Statement for Kindergartens.



3. Kindergartens will generally collect personal information about tamariki from their parents/guardians. If we need to collect personal information from another third party source – such as the Police – we should ask for the consent of the individual concerned, or someone legally empowered to decide on their behalf, before doing so.
4. Kindergarten staff, students, volunteers and contractors must read and understand the Privacy Statement for Kindergartens and be able to explain to parents/guardians or others why personal information is required, and how it may be used or shared.
5. Kindergartens must collect information in ways that are fair and not unreasonably intrusive. This requires us to consider:
 - a. The age of the person we're collecting information from. The younger they are, the less they may understand about the consequences of giving us information or authorising us to collect it from someone else.
 - b. Cultural or religious sensitivities about sharing certain information. For example, gender differences could be more important for some cultures.
 - c. The power imbalance between a teacher and a parent/guardian, or between Association staff and parents/guardians, which can have an impact on fairness.
 - d. The environment within which we're collecting information. For example, we should not ask people to reveal sensitive information on the floor of the kindergarten.
6. In some cases, Kindergartens must ask parents/guardians for their consent to collect or use personal information in certain ways. For example, we must obtain the written consent of parents/guardians in order to use photographs or videos footage of their tamariki for any public purposes, such as research, promotion, marketing, or other displays within the kindergarten.
7. Parents/guardians or whānau must not be permitted to take photographs or video footage of tamariki at Kindergartens.
8. Kindergartens must use only kindergarten devices to capture photographs or video footage of tamariki. If personal devices are used, photographs or videos must be promptly transferred to kindergarten systems and deleted from those devices.

Use and Disclosure

9. Kindergartens should generally use and disclose personal information only in the ways we outline in the Privacy Statement for Kindergartens. Any uses of information for new purposes, or disclosures to third parties not listed in the Privacy Statement for Kindergartens, must be approved by you ST and/or the Whānau Manaaki Privacy Officer.
10. Kindergarten staff, students, volunteers and contractors must confirm that the relevant parent/guardian has provided written consent before using photographs, videos or other media about their tamariki for any public purposes, such as research, promotion, marketing, or other displays within the kindergarten.
11. Kindergartens staff, students, volunteers and contractors must never disclose personal information, including photographs or videos of tamariki, on social media platforms or other





websites. For more information on acceptable use of social media platforms and other technology, see the ICT and Cyber Safety Policy.

12. Kindertartens must manage requests for information from government or law enforcement agencies, including Oranga Tamariki or the Police, in accordance with the Information Sharing Process set out at [Appendix 1: Information Sharing Guidelines](#).
13. Kindertartens must discuss the proactive disclosure of personal information to certain government or law enforcement agencies with the Child Protection Officer if they believe this is necessary to ensure the safety of a tamariki. Such disclosures should be managed in accordance with the Information Sharing Process in Appendix 1.
14. Kindertartens must manage requests from parents/guardians for personal information about their tamariki in accordance with paragraphs 15-17.

Access and Correction

15. All individuals concerned have the right to request a copy of personal information Kindertartens hold about them. This means parents/guardians, staff, volunteers, students and contractors can request a copy of personal information about themselves. These requests must be handled by the SHT or HT, and in consultation with the People Team if appropriate, and managed in accordance with the principles within the Privacy Policy and this set of procedures.
16. The Privacy Act does not give parents/guardians an enforceable right to request a copy of the personal information we hold or create about their tamariki. In practice, we will share personal information about tamariki with their parents/guardians, both on request and proactively as part of our ongoing operations. However, we must always take into consideration the best interests of our tamariki. There may be circumstances in which it is not in the best interests of the tamariki for us to release personal information to their parent/guardian (for example, where we have documented suspicions of child abuse or neglect). In these cases, you must discuss the situation with your ST, the Child Protection Officer and/or the Whānau Manaaki Privacy Officer and we may choose to refuse the release of personal information to parents/guardians.
17. It should be noted that parents/guardians have access to a secure online learning profile which contains written and visual materials about their tamariki experience while attending the kindergarten. Information in this forum will never be withheld for parents and whānau except in the most exceptional cases.

Retention and Destruction

18. Personal information must be retained in accordance with the Retention and Destruction Policy.
19. Where the Policy does not specify a retention period for a specific type of personal information, Kindertartens must ensure that the information is not retained for longer than we have a lawful purpose to use it. In some cases, the information we hold is subject to legislative retention requirements. For example, the Early Childhood Education Regulations 2008 require us to retain tamariki enrolment forms for 7 years, but that we may not retain tamariki Birth Certificates at all.





20. The disposal of any private or sensitive information held by kindergartens must be undertaken by either shredding, removing-deleting online information or depositing material in the special disposal bins held at the association offices which is collected on a regular basis by a specialist disposal company.

Security

21. All Kindergarten staff, students, volunteers and contractors must take reasonable steps to protect the personal information we hold from loss, unauthorised access, use or disclosure, or any other misuse.
22. Kindergarten staff, students, volunteers and contractors must ensure that they access and use only the personal information they need to discharge their lawful functions.
23. Personal information must be stored securely, in lockable cabinets, or in the secure system of record for that type of information. Some employment information is stored by Whānau Manaaki's HR Services in their secure systems.
24. Personnel files for Kindergarten staff, students, volunteers and contractors may only be directly accessed by the Head Office People Team. Where necessary, personal information about staff, students, volunteers and contractors may be made available to other authorised teaching or administrative staff, or third parties required to conduct audits, such as the Ministry of Education or Education Review Office.
25. Privacy breaches must be reported immediately to the SHT or HT and the ST. The Whānau Manaaki Privacy Officer is responsible for ensuring that privacy breaches are managed in accordance with the Whānau Manaaki Privacy Breach Management Procedures. Complaints from parents/guardians or whānau about privacy issues should also be reported in the first instance to the SHT or HT.

Definitions

The following definitions apply to this policy:

Parent/guardian

The adult/s who is responsible for the upbringing and care of their tamariki. This could include a parent acting as a sole guardian, and anyone else the Family Court has appointed as a guardian. For more information on who could be a guardian, check the [Ministry of Justice website](#).

NB: Not all whānau of a child are considered legally responsible for their tamariki. Ensure that the person you are dealing with on all privacy or personal information matters has the authority to engage.

Individual Concerned

Any natural person about whom Whānau Manaaki collects and holds personal information and includes tamariki, parents and whānau, staff members, contractors, any other persons listed in a child's enrolment and visitors to any Whānau Manaaki locations or online sites.

Personal Information

Any information, whether electronic or hard copy, about a individual concerned, whether or not the information directly identifies the individual concerned, and includes but is not limited to contact, demographic, health records (including ACC), qualifications information, CCTV footage, staff





performance information, emails and other correspondence, and opinions about the individual concerned.

Privacy Breach

An event (whether intentional or unintentional) in which personal information is lost or is accessed, altered, disclosed or destroyed without authorisation, or is at increased risk due to poor security safeguards, including but not limited to:

- a. accidental disclosure of personal information to the wrong recipient;
- b. employee browsing of personal information without a legitimate business reason;
- c. an external attack on a Whānau Manaaki system; or
- d. a lost or stolen Whānau Manaaki device or document.

Privacy Framework

The collective body of information that governs Privacy for Whānau Manaaki. It includes this policy and any procedures, standards or guidelines issued to support it.

Privacy Statement

A notice Whānau Manaaki has provided to a particular category of individuals concerned that outlines in general the matters set out at paragraph 4 of this policy and includes the Privacy Statements specifically designed for parents and whānau, contractors, our people and for research purposes.

Whānau Manaaki Member

Includes the Governance Board, staff members, volunteers, TONI Home Educators, and contractors working for and on behalf of Whānau Manaaki and, for the purposes of this Policy, includes any persons collecting or processing personal information in the course of research, or who are otherwise permitted access to personal information held by Whānau Manaaki.





Key relevant documents

- [Privacy Act 2020](#)
- [Education \(Early Childhood Service\) Regulation 2008](#)
- [Health and Safety in Employment Act 1992](#)
- [Children's Act 2014](#)
- [Oranga Tamariki Act 1989](#)
- Privacy Statement for Parents and Whānau
- Privacy Statement for Our People
- Protected Disclosures Policy
- Whānau Manaaki Privacy Framework
- IT Acceptable Use Policy
- IT Security Policy
- Records Management Policy





Appendix 1: Information Sharing Guidelines

General Guidelines

In some cases, Whānau Manaaki may be requested to, or decide to, share personal information about our people or tamariki with government agencies.

Where such disclosures are required or permitted by another law (such as sections 15 or 66 of the Oranga Tamariki Act), these will not breach the Privacy Act. Where no other law applies, then we must ensure that an exception to principle 11 of the Privacy Act (which relates to disclosure) applies to permit us to share the information.

Responding to requests for information from government agencies

Whānau Manaaki may receive requests for information about our people or tamariki from various government agencies, including the Police, the Ministry of Education, or Oranga Tamariki. These requests must be managed in accordance with the following steps.

1. **Escalate the request** – Requests for information from government agencies must be escalated to the ST, Child Protection Officer and/or responsible SLT Member.
2. **Verify that the request is genuine** – Ensure that the request has been received in writing from a valid agency email address or on agency letterhead. If in doubt, contact the agency using publicly available phone number to verify the request.
3. **Confirm the legal basis for the request** – Ensure that the request states the specific legislative provision it is being made under. For Oranga Tamariki, this will usually be section 66 of the Oranga Tamariki Act. If there is no legislative basis for the request, then Whānau Manaaki will need to ensure the disclosure is permitted by the Privacy Act (see below).
4. **Clarify the request** – Before making a decision on a request, we need to be clear about:
 - a. The scope of the request – how much information is the requester asking for, about whom, in relation to what time period, etc?
 - b. The purpose for the request – is it made as part of a child welfare concern or investigation, or as part of legal proceedings?
5. **Limit the scope of the disclosure** – Remember, we should only ever disclose the minimum amount of personal information required to meet the purposes of the request. Always ensure that information provided is objective, impartial and factual, and that the information is not hearsay (information gained or acquired from another and not part of one's direct knowledge).

Proactive disclosures of information to government agencies

Remember, Whānau Manaaki can always disclose personal information to third parties in the ways we outlined in our Privacy Statements. However, situations may arise in which we believe it is necessary to disclose information in ways that our people, parents/guardians or whānau might not expect.

Reporting suspected child abuse

Section 15 of the Oranga Tamariki Act states that, if we believe that a child or young person has been, or is likely to be, harmed, ill-treated, abused, (whether physically, emotionally, or



sexually), neglected, or deprived, or if we have concerns about the well-being of a child or young person, we may report the matter to Oranga Tamariki or the Police.

Sharing other safety concerns

In cases where section 15 of the Oranga Tamariki Act will not apply – for example where we need to disclose information to Police regarding our people or a member of a child's whānau – principle 11 of the Privacy Act permits us to disclose personal information if we believe on reasonable grounds that it is necessary to prevent or lessen a serious threat to health or safety.

To rely on this exception, we need to:

- be satisfied that a serious threat exists; and
- believe on reasonable grounds that disclosure is necessary to prevent or lessen that serious threat.

To decide if a threat is serious, the Privacy Act requires us to consider:

1. The likelihood of the threat occurring – is there a good chance this thing will happen?
2. The severity of the consequences if the threat occurs – if it happens, how bad will it be?
3. The time at which the threat might occur – how soon could this happen?

We also need to make sure we disclose personal information to a person or agency that can actually do something about the threat. This might be the Police, a member of a child's whānau, a healthcare provider, or an emergency healthcare provider. We cannot use this exception to disclose information to the media or any other person or agency that does not have a role in protecting people or the person concerned.

Remember, we should only ever disclose the minimum amount of personal information required to assist with preventing or lessening the threat.

Keep a record of all disclosures

In the event of a complaint to the Privacy Commissioner, we must be able to demonstrate that we had a reasonable basis to believe we could disclose personal information at the time we disclosed it. This means we must keep a record of all disclosures made under this procedure, which includes the following information:

1. Date of the disclosure
2. Details of the person or agency to which the information was disclosed
3. Copy of the request
4. Record of reasons for disclosing the information
5. Copy of any advice received about the disclosure
6. Record of what information was disclosed