Privacy
Noho Matatapu

Version 2.1 | Mahi Tuarua
Effective Date | Whakamana tahito: August 2023 | Akuhata 2023
Next Review | ā houanga arotake: August 2025 | Akuhata 2025
Policy Owner | Rangatira Kaupapa Māhere: Chief Executive Officer
Key Accountabilities | Ngā Takonga Tuatahi: Chief Operating Officer

Introduction | Tīmatanga Kōrero

Purpose

The purpose of this policy is to:

- To acknowledge the information privacy principles contained in the Privacy Act 2020.
- 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

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.

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.

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

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

Definitions | Whakamāramatanga

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.

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

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

1. Whānau Manaaki workers must collect, or must design a process or system to collect, only the personal information they need for a lawful purpose.
2. Where a process or system can operate without the collection of personal information, Whānau Manaaki will be permitted to use it anonymously.
3. 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.

4. 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.

5. 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.

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

6. 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.

7. 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

8. 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.

9. 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.

    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.

10. 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.

11. 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.

12. 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.

13. Principles relating to Māori Data Sovereignty, tikanga and mana supporting narrative are critical considerations in use and disclosure decisions.

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

Access and Correction

14. 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.

    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.

Security and Retention

15. All Whānau Manaaki workers have a responsibility to protect the personal information they handle against loss, misuse, or unauthorised access, modification or disclosure.

16. 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.

17. 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.

18. 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.

19. 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

20. 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.

21. 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.

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

c. ensure that culturally appropriate practices are embraced and applied, and are considered carefully in use, dislosure, access, retention, security and breach management decisions.

22. 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.

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

Related Procedures or Processes and Documents | Pākanga Tukanga me Pukapuka

Privacy Statements (Contractors, Our People and Parents and Whānau)
Privacy Procedures (Breach Managements, Kindergartens, Our People, Etu Ao)
File Management Policy
Complaints and Concerns Policy
ICT and Cyber Safety Policy.
Disciplinary and Misconduct Policy
Retention and Destruction Policy
Privacy Breach Management Procedures

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

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

amendments will be considered by the policy Working Group and will need to be approved by the Senior Leadership Team and/or the Board. The policy will continue on the same review cycle.

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

Breach Management | Whakahaere Takahi Tūmataiti

Version 2 | Mahi Tuarua
Effective Date | Whakamana tahito : August 2023 | Akuhata 2023
Next Review | ā houanga arotake: August 2026 | Akuhata 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 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.

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.

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

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.

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

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.

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

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

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

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. This must be within 72 hours. 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.*

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

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

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

- 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.

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

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 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.

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