PRIVACY & CONFIDENTIALITY POLICY AND PROCEDURE

POLICY

The purpose of this policy is to provide guidance to Employees, Volunteers (e.g., trustees, student placements), and/ or Contractors, of their obligations to maintain the Privacy and Confidentiality Principles of ALL personal information, as per the Privacy Act 2020

The new 'Privacy Act 2020' controls how organisations such as Te Pā collects, uses, discloses, stores, provides access to, or the correction of, personal information. As such, the organisation will ensure all personal information is kept confidential, by use of a variety of robust security measures.

In addition to the Privacy Act 2020, any organisation within the Health Sector, or that is funded by Ministry of Health (M.o.H), or a local District Health Board (DHB), must follow the requirements listed within the 'Health Information Privacy Code 2020'.

This Policy is to be read in conjunction with the 'Oranga Tamariki Act 1989' (latest version), ***Section 65A to Q – Information Sharing.*** The Principles relating to 'Information Sharing' under the Oranga Tamariki Act, differ from those of the Privacy Act, where the wellbeing of Children and/ or Young Persons at Risk, over-rides some of the Principles contained within the Privacy Act.

The 'Privacy Act' and the 'Health Information Code' 2020, ensures Te Pā maintains their commitment of obtaining, using, disclosing, and storing personal information in both a sensitive manner, and is secured in a format specific to how the information was initially received in. This will be explained in further detail within the Procedural section of this Policy.

PROCEDURE

The procedures, within this policy covers 7 categories, outlining the requirements of both the Privacy Act and the Health Information Code 2020 respectively, which are as follows:

1. Responsibilities (including those of the Privacy Officer).
2. Collection and use of Personal Information (adults, children, and young persons).
3. Disclosure and Sharing of Personal Information.
4. Access and Correction of Personal Information.
5. Storage/ Security of Personal Information.
6. Destruction of Personal Information.
7. Breaches of Privacy and/ or Confidentiality.

1. RESPONSIBILITIES

Everyone working at Te Pā has a responsibility to ensure **ALL** forms of Personal Information is kept private and confidential, at all times!!

Roles and Responsibilities of a Privacy Officer:

In **Section 201 of the Privacy Act 2020**, Te Pā must have an appointed 'Privacy Officer' (PO), whose responsibility is:

a. To ensure Te Pā complies with requirements within the 'Information Privacy Principles (IPP)' listed in the Privacy Act, and the 'Health Information Privacy Code 2020.

b. To assist the CEO in resolving Complaints received by Te Pā, or the Privacy Commissioner's Office, relating to breaches in Privacy - ***as per Part 5 of the Privacy Act 2020.***

c. To handle any personal information requests received from Tangata, Employees, Volunteers or Contractors, *as per* ***Part 4 of the Privacy Act 2020***.

The 'Privacy Officer' must ensure all personnel at Te Pā understands the requirements associated with the 'Privacy Act' and the 'Health Information Code', to prevent breaches from occurring. In some instances, an individual Employee may be solely liable for a potential breach or breaches of the Act.

As such, **ALL** Employees, Volunteers (including Trustees, Student Placements), and Contractors, of Te Pā must sign a 'Confidentiality Agreement' prior to commencement of their roles.

2. COLLECTION & USE OF PERSONAL INFORMATION

The way in which Te Pā collects/ utilises 'Personal Information', must align with the requirements stated within **Part 3 of Privacy Act,** where the collection of 'Personal Information' is only to be collected/ utilised for the purpose in which it was intended to be obtained for.

Personal information collected by Te Pā, is determined on the nature of the relationship with the person whose information we are collecting. **For Example**, Employee information would be specific to employment, and Tangata information would be specific to the service they engage with.

2.1 Who do we Collect your Personal Information from?

a. From you personally, when you provide us with your personal information as part of your employment or engagement into Te Pā.

b. Through any contact you have with us (e.g., telephone calls, emails, postal mail etc.).

c. Third parties, where you have authorised collection of your personal information by Te Pā from another agency, e.g., the Police, Department of Corrections (DOC), or where your information is publicly available.

When collecting any form of 'Personal Information', Te Pā must inform you of the reason for your information being collected.

d. **For Employees** – this should be verbally via telephone (or in person), as part of your recruitment process, and must be disclosed as part of your Individual Employment Agreement (IEA).

e. **For Tangata** - this should be verbally from your Kaiārahi as part of your Service Engagement, and in writing, as part of your enrolment, via the Referral form.

2.2. Collection of Health Information

Collection of any 'Health Information' must align with both the 'Health Information Privacy Code' and the 'Privacy Act', ensuring the Health & Wellbeing of our Employees and our Tangata. Health related personal information may include the following examples:

a. **Employees** – medical certificates, accident reports, recordings, photographs, or information relating to payroll, billing, or subsidy entitlements etc. (e.g., ACC Payments).

b. **Tangata** – medical and/ or treatment history, dependent on the Service Contracts Te Pā has in place at that time of enrolment, or as part of a Risk or Needs Assessment completion.

The collection of information from the tangata, their health provider, or a government agency, is for the purpose of their safety, or that of others within the service, Te Pā, or the wider community.

2.3 How your Personal Information is Used?

Te Pā will use your personal information to:

a. Verify your identify, when applying for employment, or enrolment into our services.
b. Undertake staff pre-employment checks or ensure you as a contractor are reputable.
c. Improve the delivery of services we provide to you, as our tangata.
d. Communicate with you electronically (e.g., via phone, text or email), when we need to make contact be it work/ service related, or to have work completed e.g., by our contractors.
e. Respond to communications from you, including communications resulting in a complaint.
f. Conduct research and/ or to produce statistical data on staff or tangata, anonymously.
g. Protect or enforce our legal rights, investigate incidents, any breaches, or complaints.
h. For any other purpose as authorised by YOU, which is not included in the examples above, or falls within one of the Principles listed within the Privacy Act 2020.

3. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

Instances of Sharing/ Disclosing of 'Personal Information' within Te Pā occurs:

a. As part of your recruitment process, including your contact information, your Curriculum Vitae (CV), or your emergency contact information.
b. As part of completing the 'Police Vetting' process for new staff, volunteers (students).
c. With training providers, as part of your 'Professional Development' journey.
d. When tangata engage within our services.
e. As a part of enrolment of tangata within other agencies such as CADS (Community Alcohol and Drug Services), or other Health Providers.
f. With businesses that support our staff and services, e.g., maintenance of our IT Systems, Data Services/ Bases, and/ or our Intranet or Website.
g. When Te Pā works with rangatahi or tamariki, where providing service requires personal information from family/ whānau, and/ or consent.
h. Personal information relating to Children or Young Persons must be in alignment with ***Sections 65A – 66Q of the Oranga Tamariki Act 1989.***

Te Pā may need to Share your personal information with other agencies, which could include:

i. The NZ Transport Agency for Traffic Fines, Contract Funders, Auditors, some Ministries, such as the Ministry of Education, or Ministry of Social Development etc.
j. Other persons authorised under the Privacy Act such as The Police, Department of Corrections (DOC), Oranga Tamariki etc.
k. Any other person authorised by **you**, under the 'Privacy Act/ Health Information Code 2020'.
l. Any business that supports Te Pā and our services, and who may be located outside of New Zealand, meaning that your personal information is being held/ processed overseas.

An example could include 'Cloud Storage of Information', as most organisations/ companies who utilise 'Cloud Based Storage', are located outside of New Zealand.

3.1 Reasons for Te Pā to Refute Access to Personal Information

Te Pā has the right to Refute access to personal information, which may include:

a. Where the disclosure of personal information would involve unwarranted disclosure or potential prejudice of another individual, within the same organisation.

b. Where disclosure of information would pose a serious threat to the health, safety, or life of another individual, or to the health and safety of the general public.

c. Where disclosure could create a significant likelihood of serious harassment to an individual.

Or, where disclosure of information relates to another person who is the victim of an offence, or an alleged offence, that could result in distress, loss of dignity, or injury to their feelings.

d. Where material is used for the purposes for determining the suitability or eligibility of employment/ appointment within Te Pā.

e. Where information was obtained from an evaluation purpose and contains identifying information of another person, or the person who supplied the evaluation.

f. Where a tamariki or rangatahi discloses situations of potential or actual abuse occurring.

g. Where a tamariki or rangatahi is seen to be being neglected or maltreated, Te Pā has the right not to disclose information shared by that tamariki or rangatahi with the legal parent, or guardian, whilst an investigation occurs with Police and/ or Oranga Tamariki.

4. ACCESS & CORRECTION OF PERSONAL INFORMATION

4.1 Accessing or the Refusal to Personal Information

In most circumstances, you have a right to access personal information held by Te Pā**.**

When requesting Access or the Correction of Personal Information, where said information is not readily available.

a. Requests are to be made in writing and submitted to the Privacy Officer at Te Pā.

b. If granted, Te Pā will require evidence to confirm that you are the individual of whom the personal information belongs too.

c. Where a request is received via a representative on your behalf, this request will need to be verified by you.

d. Te Pā has **20-Working Days** to decide and respond back to you on whether or not the personal information requested by you can be made available.

e. If a request is rejected, the Privacy Officer will provide the reason as to why your Personal Information has not been made available to you.

4.2 Correction of Personal Information

You also have the right to Correct any ready retrievable personal information held by Te Pā, where examples include:

a. A tangata meeting with their Kaiārahi has changed their phone or email address, or an employee has moved houses. Both these corrections can be made at time of request.

b. If a request for personal information has been granted by the Privacy Officer, or Te Pā, the recipient may ask if there are any changes needing to be made to personal or contact information, ensuring that information held is current and correct.

c. More lengthier corrections to personal information will require written submission to the Privacy Officer at Te Pā.

5. STORAGE/ SECURITY OF PERSONAL INFORMATION

Personal information may be stored electronically or in hardcopy formats. Te Pā will ensure your personal information is secure, regardless of the format in which it was obtained.

a. All reasonable steps to protect your personal information from being misused, lost, interfered with, or subject to unauthorised access, modification or disclosure, are taken by Te Pā.

Personal information is stored by Te Pā in secure databases, in restricted access drives, folders and files, which are backed up to 'Cloud-Based Servers' located offsite. These are maintained by our IT Specialist.

Te Pā uses industry security standard controls to effectively manage risks to the privacy, confidentiality, and integrity of all personal information.

b. All new Employees are allocated unique personal logins/ passwords and access to network drives, files, and folders, as determined by the role of the Employee and the Manager.

c. Personal information held within Employee/ Contractor/ Tangata or Financial databases, are accessed via secure logins and passwords, where access restrictions are based on the role of the Employee and data is backed-up daily onto Cloud-Based Databases.

d. Employees are required to activate the 'Lock Screen' mode on Laptops or PCs, when unattended, or to completely shut them down, when not in use.

Hard Copy information when received is retained in secure lockable filing cabinets, drawers, or cupboards, within lockable offices. Hard copy documents are scanned and uploaded to a secure drives and folders, as a means of risk mitigation.

Keys to filing cabinets/ drawers are held by the owners, where spares are held with the Service Manager, or a person of trust within another lockable cabinet or drawer, within another locked office.

Employees are reminded to turn copies of documents containing personal/ sensitive information, face down on their workstations when unattended, or locked away safely, until they return.

All printers/ photocopiers should be checked daily and cleared of sensitive materials, by shredding, or by use of the document destruction bin/s.

NOTE: When working remotely Employees have a responsibility to ensure personal information is kept confidential, by maintaining the security principles as outlined above.

6. DESTRUCTION OF PERSONAL INFORMATION

Any personal information held by Te Pā that is no longer required for the purpose it was intended, will be archived, deleted, or destructed from use, unless prevented to do so, due to legislative requirements.

Personal information pertaining to **Healthcare** will be **retained for 10-Years** (or as per legislation at time of publication of this policy). Personal Financial Information (e.g., invoices, payslips, timesheets), will be **retained for 7-Years**, or as per current legislation.

Information will be retained in hard or soft copy (dependent on specified legislation).

a. **Soft copy** information to be held in an archived section of a database, drive or folder and named accordingly, with date any identifying information, until permanent deletion.

b. **Hard copy** information to be stored within a 'Document Archiving Company', or in a secure Storage facility, where information can be easily identified and retrieved if required, until such time it can be destroyed, dependent on the specific legislation.

7. PRIVACY BREACHES

Breaches in Privacy or Confidentiality is when there have been unauthorised or accidental access to personal/ sensitive information, or an unauthorised disclosure or an unrequested alteration has occurred, or when personal information is lost, or destroyed.

A breach can also include situations where an organisation or business is prevented from accessing information, either on a temporary or permanent basis, via illicit means. These instances are often associated with a Malware Attacks or when a Security System has been breached.

Breaches in Privacy of personal / sensitive information can lead to serious harm, and could include:

a. Physical harm, threats or intimidation of another person.

b. Financial fraud that includes unauthorised transactions involving a credit card, or credit fraud.

c. Family violence, resulting in psychological or emotional harm.

The Privacy Officer for Te Pā must been notified as soon as is practically possible of any type of 'Privacy Breach', so the appropriate notification and action can be undertaken.

Breaches to Privacy are taken Seriously by Te Pā, and could result in disciplinary action, including Termination of Employment, or even Criminal Charges.

The Privacy Officer at Te Pā is currently: The Chief Executive Officer (CEO), for Te Pā

Related Policies

- *Misconduct or Serious Misconduct Policy and Procedure*
- *Copyright and Intellectual Property Policy and Procedure*
- *Complaints and Official Inquiries Policy and Procedure*
- *Interest Policy (Conflicts) Policy and Procedure*
- *Social Media Policy and Procedures*
- *Media Policy and Procedures*
- *Cyber Security Register*

Supporting Documents/ Forms/ Legislation

- *Privacy Act 2020*
- *Oranga Tamariki Act 1989 – 1 July 2022*
- *Social Sector Accreditation Standards – Level 2*
- *Confidentiality Agreement*
- *Individual Employment Agreement*
- *Tangata Service Referral and/ or Enrolment Form*
- *Tangata OR Employee Consent form*