Protection of privacy

"My privacy is respected and I understand why my information may be shared."

Intent

We collect and manage a range of personal information. We treat it respectfully and carefully, are open with people about why we collect it, how it is held and stored, what we do with it and rights of access.

We comply with regulatory standards and only release and share information in accordance with our policies and the law. Wherever possible, we forewarn and seek consent from people about when their information may have to be disclosed.

Definitions

“Personal information” is information about an identifiable, living human being. It includes health information and all other types of information whether paper, digital, or electronic which identifies a person.

Responsibilities

Management will:

- act as or delegate the responsibilities of Privacy Officer to kaimahi/staff
- monitor and manage our information management system

- monitor and manage our privacy and data breach risks with appropriate safeguards
- manage privacy and data breach incidents.

The Privacy Officer(s) will:

- monitor the organisation's compliance with this policy and the Privacy Act 2020
- assist with privacy-related training of staff/volunteers
- liaise with the Office of the Privacy Commissioner as necessary.
- support staff and volunteers when dealing with privacy-related issues.

Staff/kaimahi and volunteers will comply with this policy.

Requirements

Personal information will only be collected when necessary for service provision and business purposes.

Information will be collected in a way that is sensitive to a person's culture, age, abilities, level of understanding and circumstances.

Informed Consent will be obtained and all due care taken to ensure the person understands the reasons for collecting the information, how and when it will be used, stored, accessed, and shared, and their rights to access and correct it. (For this purpose, parental/guardian consent will be obtained before consent is obtained from a young person - see Informed Consent policy).

Source of personal information

If non-identifying information would achieve the same purpose as personal information, non-identifying information will be collected and used instead.

Where possible, personal information will be collected directly from the person concerned or their representative.

If health information is collected from a third party, the accuracy of the information will be checked with the person to whom it relates or their nominated representative.

Personal information collected from third parties for recruitment and other HR purposes (eg background and police checks) is used for evaluative purposes and not checked for accuracy.

Use of Personal Information

Personal information will only be used or shared for the purposes for which it was collected or as allowed by law (HIPC Rule 10; IPP 10 Privacy Act).

Before it is used or shared, the information will be checked (with the person concerned or their nominated representative) to ensure it is accurate, up to date, complete, relevant, and not misleading.

Safety concerns associated with use should be raised and resolved with management before using the information.
Staff/kaimahi must seek approval from the Privacy Officer/Management before using personal information for purposes that are not directly related to rangatahi service delivery.

Accuracy

A person may request a correction to their personal information/ health information.

If the correction is agreed, it must be documented in the file notes. A printed copy of the change will be given to any other party who holds the notes that require correction.
A refusal to make a correction will be documented in the relevant file with reasons. On a staff member's or young person's request, the proposed correction may be placed on their file (ie without the correction made).

People will be informed in writing about who will have access to their personal information.

Access to personal information

A person may request access to their own or their child's personal information. Unless there is good reason to refuse, we will facilitate access as follows:

- enable access within 20 working days of receiving the request for access
- remove information about another person on their file beforehand (under the oversight of management/their delegate)
- encourage the person to have support while viewing their record (ie for sensitive information)
- inform the person of their right to seek a correction to their personal information.

A parent/guardian may access their child's personal information on request unless we reasonably believe it would be contrary to the young person's best interests after considering:

- the young person's views about the access
- the nature of the personal information to be accessed
- the parent's reasons for wanting access
- the importance of privacy to the wellbeing of the rangatahi.

If access is denied, the parent/guardian will be informed of our reasons and their right to complain to the Privacy Commissioner.

Recordkeeping

A record will be kept of:

- any request for access and of the date when received
- a copy of the information accessed
- authorisation to access (if given by a person relevant)
- the reasons for delay or refusal (if applicable)
- safeguards implemented to action the request
- other steps taken for the request (eg in relation to parental access).

Privacy officer

We have a Privacy Officer to support our compliance with the law and policies and to support our interactions with the Office of the Privacy Commissioner (eg about privacy breaches; complaints etc.)

Compliance

Social Sector Accreditation Standards - Level 2 Client services and programmes 5.0; Governance and management structure and systems

Social Sector Accreditation Standards - Levels 3 & 4, Governance and management structure and systems 2.0

NZS 8134:2021 Criteria 2.5, 1.4

Review

Date: July 2022

Next review: by June 2024

Information safeguards

"They look after my personal information."

Intent

We take the job of safeguarding personal information seriously. We monitor risks to data security and implement measures to address these risks in line with good practice.

This policy prescribes minimum operational and electronic safeguards. We will vary these safeguards to ensure we respond to new and emerging risks. For information safeguards when working remotely, including when working from home, see IT and Personal Devices (BYOD) policy.

Definitions

"Information" in this policy involves personal and organisational information.

"Personal information" is information relating to an identifiable person including hard copy, digital and electronic information. It includes health information.

"Organisational information" refers to information about our business affairs whether stored in hard copy, digitally or electronically.

"Unique identifiers" are individual numbers, references, or other forms of identification allocated to people by organisations eg driver's licence and passport numbers; the NHI number assigned by Ministry of Health for health services.

Requirements

Privacy and data security training

Kaimahi will be trained in privacy and data security good practice.

The Office of the Privacy Commissioner's 'Privacy ABC' or an equivalent level of training should be completed at least every two years https://elearning.privacy.org.nz/

Operational safeguards

The following safeguards will be adhered to:

- information will only be accessed if authorised and as-necessary (based on role and responsibilities)
- personal information will not be discussed or stored in public areas
- paper records will be scanned and stored electronically. If this is not reasonably practicable, paper records containing personal information will be kept in a secure place (eg locked filing cabinet)
- records relating to a rangatahi known or related to a staff member/kaimahi will be kept confidential from the staff member concerned
- when kaimahi/others leave the organisation, their email address will be disabled and their emails and calendar appointments archived
- rangatahi, /staff and others' personal information will not be kept on personal laptops or home PC
- when sharing information, all due care will be taken to transmit the information securely:
    - check the physical and electronic address of the recipient before sending
    - comply with electronic/database transfer protocols

    - send the information to a named authorised person in the safest and most confidential way eg use a tracked courier for physical transfer of a person's record - copy or original.
- if it is necessary to remove personal or confidential information from the premises, the information must be kept secure (eg personal information carried in a locked bag)
- user accounts, passwords and system access will be regularly reviewed.

Accessing personal information other than for authorised and professional purposes will be treated as a disciplinary matter.

Electronic record safeguards

Personal information will be held and stored electronically with appropriate safeguards in place, including:

- password/login system for secure access
- access only on an authorised, and as-necessary basis
- a screen saver programme to minimise risk of unauthorised access to files
- safeguards when using cloud services (eg monitoring and limiting file shares)
- regular back-up of records with recovery of information from the back-up tested regularly
- where possible, workstations and computers are positioned to avoid personal information on screens being seen by unauthorised people
- terms and conditions of software, including cloud-based CMS, are complied with
- a person's data is not left on an unattended screen or left open when other people are present
- user accounts, passwords and system access rights are reviewed regularly (at least once every six months)
- staff comply with instructions to safeguard IT hardware and devices and compliance is monitored
- anti-virus software is installed and run regularly.

Passwords

Passwords are not to be shared and should conform to NZISM 2015 complexity rules:

- a minimum password of 16 characters with no complexity requirement; or
- a minimum password length of ten characters, consisting of at least three of the following character sets:
    - lowercase characters (a-z)
    - uppercase characters (A-Z)
    - digits (0-9)
    - punctuation and special characters.

Unique Identifiers
A unique identifier or reference will be assigned only if necessary (for protection, efficiency and/or continuity purposes). Reasonable care will be taken to protect unique identifiers from misuse.

No one will be asked to disclose an identifier assigned by another agency unless we are wanting it for the original reason it was assigned (eg health reasons).

Risk management

Privacy risks will be monitored and regularly reviewed. Safeguards for new and emerging risks will be implemented that are proportionate to the level of risk we identify.

Risks and measures taken to address risks will be recorded in the organisational risk register.

The Privacy breach policy will be applied to prevent and respond to a breach.

Safe disposal of personal information

Personal information will be securely disposed of once the purpose for which we collected it no longer applies and provided we are not required by law to keep it (eg health & disability requirements; wages records) or the person/whānau to whom it relates does not want it.

Reasonable care will be taken to safeguard privacy during the destruction process. Records on our computer hardware and any backup of the records will be wiped in such a way as to be unable to be reconstructed in any way.

Virus protection

All due care must be taken to avoid the risk of computer virus transmission:

- avoid opening 'executable' files (those ending in .exe) and other files (.com, .vbs etc.) that are known to transmit viruses via attachments to emails
- avoid opening email if in doubt about the contents
- disable macros in Office and Excel
- ensure that anti-virus software is run and updated at least weekly.

Review

Date: July 2022

Next review: June 2024

Information sharing

"My information is treated and shared respectfully and only if necessary."

Intent

We are kaitiaki of people's information and respect the trust and expectations of confidentiality that rangatahi and staff/kaimahi have of us in our relationship with them.

We inform rangatahi and kaimahi about the limits of confidentiality and disclose their personal information to others only in accord with law and our policies.

Definitions

“Authorised agency or practitioner” in this policy refers to a family violence agency or social services practitioner.

"Child protection purpose" refers to any of the purposes outlined in section 66C of the Oranga Tamariki Act 1989.

“Family violence” is defined in section 9 of the Family Violence Act 2018.

“Family violence purpose” refers to any purpose outlined in section 20 of the Family Violence Act 2018:

- to make or contribute to a family violence risk or needs assessment
- make or contribute to a decision or plan that is related to or responds to family violence
- help ensure that a victim is protected from family violence.

“Personal information” is information about an identifiable, living human being. It includes all information whether paper, digital, or electronic which identifies a person - eg rangatahi, staff member/kaimahi, ex-rangatahi, volunteer.

General rules

The general rules are:

- people will be informed about and must consent to their information being shared with others, including with other professionals, before it is shared. Parental consent will be obtained before the personal information of a child/rangatahi can be shared

- people will be told on entry about when their personal information may be disclosed and who, in the organisation and externally (eg auditors), will have access to it
- any disclosure of personal information will only be to the extent necessary to the work/mahi and within the scope agreed with the person to whom it relates
- all due care will be taken to safeguard privacy when transferring or sharing personal information
- information about a person's associate or another person (eg partner, or parent) will be treated as confidential and will not be disclosed to others unless the exceptions below apply
- personal information obtained from third parties (eg supplied by a doctor or another health worker) will not be disclosed or shared without the consent of the person to whom it relates unless the exceptions (below) apply
- if a person does not consent to the disclosure of their personal information but the disclosure is mandated or allowed by law, their views will be obtained, considered and recorded
- if staff/kaimahi are contacted by individuals or agencies seeking a person's information and are unsure about releasing it, they should discuss this with management/senior staff before responding.

Exceptions to the rules

Personal information will not be disclosed without a person's consent unless there are reasonable grounds for believing that one of the following circumstances applies:

- the disclosure of the information is likely to assist a family violence or child protection response or plan and is to an authorised agency;
- it is specifically authorised by law (e.g., a request from Oranga Tamariki under section 66 Oranga Tamariki Act 1989)
- it is for the same purpose for which the information was obtained
- it is part of reporting concern about the well-being of a child or young person
- the disclosure is necessary (ie needed) to prevent or lessen a serious threat to:
    - public health or public safety, or

    - the life or health of the individual concerned or another individual, and
- we reasonably believe that disclosure will help to prevent or lessen the threat.
- any of the other circumstances in IPP 11(1) or Rule 11 (2) of the Health Information Privacy Code exist
- it may be disclosed to a foreign recipient under the IPP 12 of the Privacy Act/Rule 12 of the Health Information Privacy Code.

If it is safe and appropriate, we will inform a person when we share/disclose their personal information in the above circumstances.

Duty of care

Any staff/kaimahi involved in sharing another's personal information must take all reasonable care with:

- communicating and transmitting the information
- checking disclosure is authorised (eg client has given written consent to release; requestor is an authorised agency or practitioner)
- if not authorised by the person, that there is legal authority to release it
- the scope of the information (ie only information necessary to the information-sharing purpose should be shared)
- accuracy ie the information should be correctly identified as fact, opinion etc
- recording (in the appropriate file) when and to whom personal information is given and why.

Any concerns or doubts about information-sharing, should be raised with management before proceeding.

Tūtaki Youth's secure file sharing and transfer service must be used to share client information when available (eg Medtech; Sharefile).

Sharing information to lessen or prevent a threat

In addition to the above, when deciding if personal information should be shared to prevent or lessen a threat of serious harm to public or individual health and safety, the following should be considered:

- how the information will be used and its likely effectiveness (ie that the disclosure will lessen the threat)
- possible adverse consequences of sharing the information (eg loss of trust in Tūtaki Youth; on-sharing of the information by the recipient or security risks), and
- whether there are other options to address the health or safety risk that involve less privacy intrusion and less possibility of harm but would be as equally effective in addressing the risk, and
- if so whether it is possible to await the outcome of lesser measures.

Te Tiriti o Waitangi

Where Māori interests are at stake, in addition to the above, Treaty obligations and tikanga Māori must be considered. In particular, it must be recognised that the right to life and health is a "highly prized taonga"; that information-sharing about health status may, in situations where Māori health is at risk, be vital to the Treaty right of providing Kaupapa Māori options.

Record keeping

A request for personal information and how it was dealt with must be recorded on the relevant file including:

- when and with whom the information was shared or not shared
- if consent was given and if not, the person's reasons and how their views were considered
- what information, if any, was shared (or copy attached)
- the reason for the disclosure
- how the decision was made
- the reasons for sharing or refusing to disclose the information.

Compliance

Social Sector Accreditation Standards - Level 2 Client services and programmes 5.0; Governance and management structure and systems 6.0

Review

Date: July 2022

Next review: June 2024

Breach of Privacy

Privacy breaches are taken seriously."

Intent

We respond quickly and proportionately to a breach of privacy. We aim to contain and mitigate the impacts and identify and address the cause(s). We notify affected people and the Privacy Commissioner if serious harm is caused or is likely to be caused and act to prevent future privacy breaches.

Definitions

"Notifiable privacy breach" is a privacy breach that poses a risk of serious harm or causes serious harm to a person.

"Privacy breach" or "breach" involves access to or collection, use, or disclosure of personal information in contravention of our policies and the

law. It may involve deliberation, deception or occur by mistake or without fault.

Responsibilities

The board will oversee and support the management of privacy risks including the actual and likely impacts of privacy breaches.

Management will:

- manage the risks and impacts of privacy breaches including notifiable privacy breaches
- consult with and report to the board about notifiable privacy breaches and any significant privacy risks
- ensure kaimahi are trained in and able to implement this policy if a breach occurs
- ensure notifiable privacy breaches are notified to the Privacy Commissioner and affected individuals in accordance with the law.

Kaimahi and volunteers will report all breaches of privacy to management including minor breaches and comply with this policy if there is a breach of privacy.

Requirements

Containment

If a privacy breach occurs, we will take immediate steps to contain the breach, such as:

- shutting down the [breach] activity
- revoking or changing access codes
- correcting weakness in operational or electronic security.

Review for cause and impact

A preliminary review will be undertaken to identify the cause of the breach, scope the extent of it and assess the impacts on the individuals whose information it is.

Further steps to contain and manage the breach will be taken if indicated by this review.

Evidence of the breach will not be destroyed until the investigation is completed.

Notifying the Privacy Commissioner and affected individuals

Unless a legal exception applies, the Privacy Commissioner and affected individuals will be notified of the privacy breach if it has caused or is likely to cause serious harm having regard to:

- the extent to which our response to the breach has reduced the harm/risk of harm
- who is likely to receive the information as a result of the breach
- the sensitivity of the information to the individual whose information it is
- whether the information is protected by a security measure
- other relevant matters.

The NotifyUs tool will be used to help decide if a privacy breach should be notified. If we are unsure if serious harm has been caused or may be caused by a breach, management/their delegate will notify the Privacy Commissioner and be guided by their advice.

Notifications will be made within 72 hours of becoming aware of the privacy breach and will cover the following:

- when and how the breach occurred
- the nature and scope of personal information
- what's been done to control or reduce the harm
- people/agencies who have been informed about the breach
- other relevant matters.

Notifications can be made to the Privacy Commissioner here.

In addition to the above, affected individuals will be informed (eg through email, phone or in-person meeting) about the following:

- what they can do to avoid or reduce harmful impacts and to further protect themselves
- that we have notified the Privacy Commissioner
- their right to make a complaint using our internal complaints process and to the Office of the Privacy Commissioner
- how they can contact us
- the identity of the recipient of the personal information if the disclosure is necessary for safety reasons.

Public notifications

If it is not reasonably practicable to notify individuals who are or may be affected by the privacy breach and no legal exception applies, public notice will be given about the privacy breach (eg on our website etc).

Informing others

The following will also be informed of the privacy breach on as-needed basis:

- the board for all notifiable breaches and any breach posing a significant risk to the organisation
- the Police, if criminal activity appears to be involved
- any person who can assist with containing and lessening the impacts of the breach
- if relevant, our insurer
- any regulatory or professional membership organisation (if the breach involved misconduct or negligence by staff.)

Prevention

We will investigate a privacy breach, including minor breaches, to the extent necessary to ascertain:

- the cause of the breach and
- what controls are needed to prevent a future breach.

Both the investigation and controls should be proportionate to the significance of the privacy breach. The risk of future breach and the

efficacy of the controls will be monitored in accordance with our risk management and quality improvement approach.

Recordkeeping

We will be transparent about how we respond to and manage privacy breaches by ensuring that we record the steps we take and our reasoning. This will include recording our reasons for deciding to report or not report a privacy breach to the Privacy Commissioner and affected persons.

Review

Date: July 2022

Next review: June 2024