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.

"Privacy Officer"- see here for role of Privacy Officer.

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

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

When and how we collect personal information

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 *(evidenced by a Privacy Consent form or equivalent.)*

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. When personal information is collected from a third party or via an AI tool, reasonable steps will be taken to check accuracy (eg check with the person whose information it is; check reliability of AI tool for that purpose.)

However, if personal information is collected from third parties for evaluative purposes (eg referee checks) it will not be 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).

Staff should be "risk-aware" when using people's personal information.

Privacy risks should be identified and resolved, or if unable to be resolved, discussed with management, before personal information is used.

As a general rule, information collected for one purpose cannot be re-purposed. Staff/kaimahi must seek approval from the Privacy Officer/management before using personal information for purposes that are not directly related to the reason(s) for collecting the information.

Personal information will only be shared with overseas organisations and people if the same or better privacy protections apply to the receipt and use of the information in that country as in NZ/Aotearoa. Unless specifically authorised by WCM, personal information will not be input to AI tools.

Accuracy

Reasonable steps will be taken to ensure that the information we hold or use is accurate, up-to-date, relevant, and not misleading.

A person may request that personal information/ health information we hold is corrected.

If the correction is agreed, it will 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 correct will be documented in the relevant file with reasons. At the person's request, the proposed correction will be placed on their file (ie without the correction made).

Before using AI or other tools, we will check for accuracy giving known risks including:

- whether there is a risk of bias in the AI tool (eg if the tool's outputs are based solely on training data generated overseas)
- how reliable and accurate the tool is known to be when used in the way we intend
- that the personal information generated or collected by WCM through AI will be able to be corrected (on request by a person or at our initiative).

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's request to access their child's personal information may be declined if the child is under 16 years and we reasonably believe that parental access to their health information would not be in the young person's interests after considering:

- the young person's views on 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 young person/rangatahi.

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

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

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.)

AI and Personal Information

WCM will take a cautious approach to using AI and be guided by advice from the Office of the Privacy Commissioner about responsible use under the Privacy Act 2020.

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: February 2024

Next review: by January 2026