

AGE CONCERN WAIKATO

PRIVACY POLICY

Policy Statement

Your privacy is important to us (**Age Concern Waikato**). We are committed to protecting the privacy, dignity, and mana of the older people, whānau, volunteers, staff, supporters, donors, and community members we interact and/or work with.

We only collect information from you that is relevant and necessary for the support we are providing, and we do our best to make sure your information is accurate and up to date.

Purpose

This Privacy Policy explains how we collect, use, store, share, and protect personal information in accordance with the New Zealand **Privacy Act 2020** and the **Health Information Privacy Code 2020**.

Who This Policy Applies To

This policy applies to personal and/or health information we collect or hold about people who engage with us, including clients, older people seeking support, whānau and representatives, volunteers, subscribers, donors, event participants, service providers, employees, contractors, and visitors to our premises, website, or social media channels.

Collecting Your Personal Information

What Personal Information We Collect

We only collect information that is necessary for our services, programmes, or organisational operations.

Depending on the circumstances, this may include:

- **Identity information** such as name, preferred name, age, ethnicity, gender, and other relevant identification details associated with the services Age Concern Waikato provide.
- **Contact information** such as address, phone number, email address, emergency contact details.
- **Service information** such as referral details, service history, case notes, communication preferences, assessment information, eligibility information, photos, videos, support needs, goals, preferences, feedback, and complaints.
- **Health and disability information**, where relevant to providing or arranging support, activities, mobility services, exercise programmes, elder abuse response, social work, advocacy, education, or referrals.

- **Relationship and advocate information** such as information about whānau, representatives, carers, support people, attorneys, guardians, or other contacts where this is relevant to the support being provided.
- **Volunteer, staff, contractor, and governance information**, including recruitment, police or Ministry of Justice vetting, training, supervision, payroll, health and safety, and conflict of interest information.
- **Payment information** associated with donations, subscriptions, fundraising, events, and payroll.
- **Website, email, and digital interaction information**, such as online forms, emails, social media messages, cookies, device information and IP address, and analytics where used.
- **Any other information you choose to provide.**

How We Collect Personal Information

We always collect information **lawfully and fairly**.

Where practicable, we will collect information directly from the person concerned. We may collect information through:

- Direct conversations (via phone, email, SMS/text message, online chat, in person).
- Online and in-person forms.
- Observations arising from personal interactions including assessments, meetings, home visits, events.
- Online channels (e.g. websites and social media).

In some situations, we may collect information indirectly (for example when receiving a referral). This may include information from whānau, carers, health providers, social service agencies, government agencies, referrers, emergency services, or authorised representatives.

What we tell you about the information we collect

When we collect information from you, we will take reasonable steps to let you know:

1. Why we are collecting the information,
2. Who we will share it with,
3. Whether it is required or voluntary, and
4. The consequences of not providing it.

Where your information has been provided to us by another party (for example a referral to our services), unless an exception applies, we will contact you as soon as is practicable to let you know the information outlined in steps 1-4 above, as well as:

5. What information has been provided to us,
6. The name and address of the party that provided us with your information,
7. If our receipt of the information is authorised or required by law, what law that is, and
8. Your right to access and correct your information.

Storing Your Personal Information

Security

We take all reasonable steps to keep personal information safe and secure, including:

- Password-protected systems
- Secure physical storage
- Role-level restrictions for staff access
- Provision of all company equipment necessary for data capture (e.g. phone/laptop)
- Staff training on privacy obligations
- Regular review of data security practices
- Where information is no longer required to be kept, it is disposed of in a manner that preserves the privacy of the individual.

Staff, volunteers, contractors, and service providers are expected to respect confidentiality and handle information only for authorised purposes. We take extra care with sensitive information, including health information and information relating to elder abuse, vulnerability, family circumstances, safety, or wellbeing.

Overseas Disclosure and Cloud Services

Some of your personal information may be stored or processed overseas (for example where information is stored in the cloud). In these situations, we will take reasonable steps to ensure that your private information is held and processed in line with the Privacy Act 2020.

Accuracy

We take reasonable steps to ensure personal information and health information is accurate, up to date, complete, relevant, and not misleading before using or disclosing it. We encourage people to tell us when their details or circumstances change.

Retention

We only retain personal information for as long as necessary to fulfil the purpose it was collected for, or as required by law.

In adherence with the Health (Retention of Health Information) Regulations 1996, we retain health information for 10 years from the last time that services were provided to the individual, unless the file has been transferred to another provider.

Using Your Personal Information

We use personal information to:

- Provide and improve our services
- Make, receive and manage referrals to and from other agencies or professionals (where permitted in line with law and this policy)
- Assess eligibility for programmes
- Communicate with you and any authorised representatives
- Manage donations, volunteering, or subscriptions
- Meet reporting or contractual obligations
- Ensure safety and wellbeing

- Respond to requests, complaints, incidents or notifiable privacy breaches
- Conduct organisational administration

We will not use your information for any purpose that is **inconsistent with why it was collected**, unless permitted by yourself, or law.

Sharing Your Personal Information

We **do not** sell or trade personal information.

When We Share Personal Information

We will only share information:

- With your consent, or
- Where it is required or permitted by law, or
- Where there is a serious threat to health or safety.

Who We Share Your Information With

We may share personal information with:

- The individual concerned or their authorised representative
- Service partners, agencies or individuals involved in your support
- Funders or government agencies where required by contract or law, using deidentified or aggregate information where practicable
- Professional service providers and advisors necessary for our operations (e.g., technology, accounting, auditors, technology, legal, insurance), subject to appropriate confidentiality and security expectations
- Emergency services, where imminent safety is at risk

Social Media

If you interact with us on social media, content you posted may be visible to others and may be governed by the privacy settings and terms of the relevant platform.

Website Links

Our website may contain links to other sites of potential interest. If you use these links to access external websites; any personal information you provide to those sites is not managed by us. Our Privacy Policy does not apply to these sites. You should exercise caution and read the Privacy Policy of the applicable external website.

Health Information

Health Information is sensitive and is managed with particular care. We may collect health or disability information where it is relevant to delivering services safely and appropriately, arranging referrals, supporting wellbeing, assessing mobility or support needs, managing risks, or meeting legal and safeguarding responsibilities.

Where the Health Information Privacy Code 2020 applies, we will follow its rules for collecting, using, storing, disclosing, accessing, correcting, retaining, and disposing of health information. We

will usually collect health information directly from the person concerned unless it is not practicable or an exception applies. We will only use or disclose health information for the purpose collected, with consent, or where otherwise permitted or required by law.

Managing Data Breaches

We take all appropriate steps to protect your privacy; however inadvertent privacy breaches may occur despite the best practices and intentions.

A privacy breach may include unauthorised access to, disclosure of, loss of, alteration of, or destruction of personal information or health information. We will take privacy breaches seriously and act promptly to contain, assess, and manage the breach by taking the following steps:

1. Alert

Where our staff or volunteers are notified of an actual or suspected privacy breach, they will:

- Immediately take any appropriate action to stop the breach, and
- By no later than the end of that business day, notify the Privacy Officer by completing the Privacy Breach Notification Form.

2. Containment and Assessment

Within 1 business day of receipt of a Privacy Breach Notification, the Privacy Officer will work with the reporting party to review the information to assess the impact of the breach and take immediate steps to contain and minimise any further harm arising.

These steps may include:

- Investigation to fully understand the breach
- Taking action to prevent further information breach
- Where there is potential for serious harm, notifying the Office of the Privacy Commissioner, and the affected individuals within 72 hours of initial alert.

3. Evaluation and Corrective Action

The Privacy Officer will then lead a full evaluation of the breach including what, how, when, why the breach happened and who was involved in the breach. This evaluation will produce insight and actions to be taken to prevent such future breaches (where applicable).

Often, more information will come to light throughout assessment and evaluation. Where this occurs, each new piece of information will be contained and assessed under Stage 2. Any required notification will occur within 72 hours of the information being discovered.

Contacting us

Privacy Officer

Age Concern Waikato General Manager
150 Grantham Street, Hamilton Central, Hamilton 3204
PO Box 98, Waikato Mail Centre, Hamilton 3240
Phone: 07 838 2266
Email: privacy@ageconcernwaikato.org.nz

Accessing and Correcting Your Information

You have the right to:

4. Request access to the personal information we hold about you
5. Request corrections to ensure your information is accurate and up to date

To make a request, please email privacy@ageconcernwaikato.org.nz, with:

6. **Subject:** Access Request OR Correction (as relevant)
7. **Body:** Please provide your full name and date of birth so that we can align the request to your file. If you want us to correct your information, please detail what information you are requesting that we correct.

We will respond within 20 working days after the day on which your request is received.

To make a request, please contact our Privacy Officer: privacy@ageconcernwaikato.org.nz.
We will respond within 20 working days after the day on which your request is received.

Privacy Concerns or Complaints

If you have a concern or complaint with how we manage private information, we encourage you to contact our Privacy Officer who will try to resolve the matter. We will acknowledge and respond to complaints in a fair, respectful and transparent way. This may include seeking further information from you to help us understand the concern.

If you are not satisfied with our response, you can contact the Office of the Privacy Commissioner by going to their website www.privacy.org.nz

To make a complaint, please email privacy@ageconcernwaikato.org.nz, with:

8. **Subject:** Privacy Concern or Complaint
9. **Body:** Please provide as much information as possible to help us investigate. This could include who is involved, what information has been used or disclosed inappropriately, when the incident occurred, why you feel the individual's privacy rights were not upheld, and any information you have on how the incident occurred.

We will respond within 20 working days after the day on which your request is received.

Updates to This Policy

This policy will be reviewed whenever there are significant changes to our services, systems, legal obligations, privacy risks, or guidance from the Office of the Privacy Commissioner. At minimum, it will be reviewed every three years. The current policy will be published on the Age Concern Waikato Website at www.ageconcernwaikato.org.nz/privacy