

# Privacy Policy

---

## *Anxiety New Zealand Trust*

### **1) Who we are**

Anxiety New Zealand Trust also known as Anxiety NZ (we, us, our) provides mental health and wellbeing support through:

- Clinical services (eg therapy, assessment, treatment planning, clinical notes, follow up).
- Peer services (eg peer support groups, peer led wellbeing support, psychoeducation, and community based support).
- Online and in person delivery, including telephone, video, digital platforms, and face to face sessions.

This Privacy Policy explains how we collect, use, store, share, and protect personal information, including health information.

### **2) Our privacy commitments and the laws we follow**

We aim to be open and transparent about how we handle personal information and to keep it secure.

In Aotearoa New Zealand, our handling of personal information is governed by the Privacy Act 2020 and, because we provide health and disability services, the Health Information Privacy Code 2020 (HIPC).

From 1 May 2026, the Privacy Act includes Information Privacy Principle 3A (IPP3A), which introduces notification requirements when personal information is collected indirectly (from someone other than the individual).

We also aim to meet expectations under the Code of Health and Disability Services Consumers' Rights, including respecting privacy and supporting informed choice and consent.

### **3) What personal information and health information we collect**

The information we collect depends on the service you use and what is necessary for your care, support, and safety.

#### **A. Identity and contact information**

- Name, date of birth, contact details, address, preferred name and pronouns.
- Emergency contact details.
- Demographic information that may be relevant to services (eg gender, ethnicity, languages, accessibility needs).

#### **B. Health and wellbeing information (health information)**

**Version: 1.1**

- Information about your mental health and wellbeing, symptoms, goals, and history.
- Risk and safety information (including if there are concerns about risk to self or others).
- Information relevant to providing therapy or support, including session notes and clinical records (for clinical services).
- Participation information related to peer groups or peer support (eg attendance, group preferences, any safety needs).

#### C. Information about how you use our services

- Appointments, referrals, communications with us (email, phone, messaging).
- Service outcomes and feedback (where you choose to provide it).

#### D. Payments and administration (if applicable)

- Donation or payment records (where relevant).
- Invoices and receipts.

We aim to collect only what we need for a lawful purpose connected to our functions and services.

### 4) How we collect information and where it comes from

We collect information in a few ways:

#### A. From you directly (most common)

For example, when you contact us, register, book, or attend a service, complete forms, consent documents, or assessments, participate in therapy, peer support, or groups, provide feedback, or communicate with our team.

#### B. From other people or organisations (only when appropriate)

We may collect information from:

- Your GP or other health provider (eg referral letters, reports), where you have arranged this or otherwise authorised it.
- A family member, whānau member, caregiver, teacher, or observer, where you ask them to provide information, or where it is necessary for safety and support (eg an observer form).

#### C. Unsolicited information

If we receive information we did not ask for, we will only keep it if it is necessary for a lawful purpose connected to our services, and otherwise we will securely dispose of it where appropriate.

#### 4A) Indirect collection notification (IPP3A) – effective 1 May 2026

From 1 May 2026, if we collect personal information about you from someone other than you (an indirect collection), we will take steps that are reasonable in the circumstances to make sure you are aware of:

- the fact that the information has been collected,
- the purpose of the collection,
- the intended recipients of the information,
- our name and contact details (and confirmation that we hold the information),
- if the collection is authorised or required by law, which law, and
- your rights to access and request correction of your information.

#### Timing

Where we have not already provided notice in advance, we will notify you as soon as reasonably practicable after the information is collected, taking into account the context and sensitivity of the information. If notification is delayed, we will be able to explain why, and we will document our rationale where appropriate.

#### How we will notify you

Depending on circumstances, we may notify you using:

- our website privacy policy and service specific privacy notices,
- information included in referral or onboarding materials,
- brief notices on forms, supplemented by longer notices online (layered notices),
- phone scripts or email communications where appropriate.

#### When we may not notify (exceptions)

IPP3A includes exceptions where notification is not required in specific situations. These include (among others) where you have already been made aware, where notification is not reasonably practicable, or where notification would prejudice the purpose of collection in limited circumstances. Where an exception applies, we will still aim to be transparent where it is safe and appropriate.

#### Where another agency notifies on our behalf

In some situations, an organisation that deals with you directly (eg a referrer) may notify you about our indirect collection on our behalf. If we rely on this, we will seek to ensure there is evidence that you were informed of the IPP3A matters, and we may include notification responsibilities in our agreements with partner organisations.

#### People acting on your behalf

Where someone is legally authorised to act on your behalf under formal arrangements, collection from that person may be treated as direct collection and we will provide notice accordingly. Where an authorised representative provides information on your behalf outside those formal arrangements, we will generally treat that as an indirect collection and take reasonable steps to ensure you are aware of the IPP3A matters, often by ensuring your representative is given the relevant notice to share with you.

## 5) What we use information for

We use personal information and health information to:

- provide services and support, including clinical and peer services,
- communicate with you about appointments and service delivery,
- support safety and quality, including risk management and professional supervision,
- run our operations, including scheduling, records management, and internal reporting,
- meet legal and compliance obligations.

Once health information has been collected for a particular purpose, it can generally be used or disclosed for that purpose, with limits and safeguards.

## 6) When we share information and who we share it with

We treat health information as sensitive and aim to keep it confidential.

We may share information in the following circumstances:

### A. Within Anxiety New Zealand Trust

We may share information internally with staff, contractors, clinicians, and peer facilitators only on a need to know basis to provide services, ensure safety, and support quality and continuity.

### B. With your consent or at your request

With your consent (or where you ask us to), we may share information with:

- your GP, counsellor, psychologist, psychiatrist, or other health provider,
- a support person you nominate (eg whānau member, caregiver),
- other organisations involved in coordinating your care.

### C. For serious threats to life, health, or safety

In limited circumstances, we may use or disclose information when it is necessary to prevent or lessen a serious threat to someone's life, health, or safety.

### D. Where required or permitted by law

We may disclose information where required or authorised by law, including lawful requests and legal obligations.

#### E. Service providers who help us operate

We may use trusted third parties (eg secure IT providers, clinical management systems, communications tools) to store or process information on our behalf. We require these providers to protect information and only use it for the services they provide to us.

If information is disclosed outside New Zealand (eg some cloud services), we will take steps to ensure appropriate safeguards consistent with cross border disclosure requirements for health information.

We do not sell your personal information.

### **7) Consent, choice, and services for people of all ages**

We provide services to children, young people, and adults. We take extra care to explain privacy in an age appropriate way. For clinical services and some peer services, we may ask for consent to collect and share information. Where it is appropriate and lawful, we may involve parents, guardians, or whānau, while still respecting the privacy of the person receiving support.

### **8) How we keep information safe**

We take reasonable steps to protect information from loss, unauthorised access, misuse, modification, or disclosure. Safeguards may include access controls, multi factor authentication where available, secure storage systems and encryption where appropriate, staff privacy training, and secure disposal processes.

#### **8A) Systems we use**

We use Medtech Evolution as our practice management system to manage client records. We also use a deidentified workflow tracker in Microsoft 365 (Excel) that uses Medtech ID numbers only and does not include identifiable client information. Access to our systems is restricted to authorised staff and we use reasonable safeguards to protect personal information.

### **9) How long we keep information (retention)**

We only keep personal information for as long as we have a lawful purpose for using it. For health records, retention requirements apply. Health agencies must generally keep health records for at least 10 years from the last date services were provided, subject to limited exceptions (for example, where a full record has been transferred to a new provider or provided to the person). After applicable retention periods, we securely dispose of or deidentify information.

## **10) Your rights: access and correction**

You have the right to request access to information we hold about you and to request correction if you believe it is inaccurate, incomplete, irrelevant, or misleading. In limited circumstances, we may be allowed to withhold some information (for example, if providing access would pose a serious threat to life, health, or safety).

How to make a request

Email or write to our Privacy Officer (details below). We may ask you to verify your identity before releasing information.

## **11) Privacy breaches**

If a privacy breach occurs, we will take steps to contain it, assess risks, and reduce harm. Where a breach is a notifiable privacy breach, we will notify the Privacy Commissioner and affected individuals as required.

## **12) Using our website and online services (cookies and analytics)**

If you use our website or online services, we may collect basic technical information such as IP address, device type, browser type, and pages visited. We use this to maintain security, understand usage, and improve services. You can usually control cookies through your browser settings.

## **13) Deidentified information, research, and service improvement**

We may use deidentified or aggregated information (where individuals are not identifiable) to improve our services, report to funders or partners about service volumes and outcomes, and evaluate programmes. If we wish to use identifiable information for research or publication, we will seek appropriate consent and follow applicable ethical and privacy requirements.

## **14) Unique identifiers (eg internal client IDs)**

We may assign an internal identifier to help manage records accurately. We take steps to prevent misuse of identifiers and follow applicable privacy requirements.

## **15) How to contact us (Privacy Officer) and how to complain**

Privacy Officer

Anxiety New Zealand Trust

Email: [reception@anxiety.org.nz](mailto:reception@anxiety.org.nz)

Phone: 09 846 9776

Postal address: 77 Morningside Drive, St Lukes, Auckland 1025

If you are not satisfied with our response, you can complain to the Office of the Privacy Commissioner.

#### **16) Changes to this Privacy Policy**

We may update this policy from time to time to reflect changes in our services, systems, or legal requirements. We will post the current version on our website and update the effective date.

Effective date: 12<sup>th</sup> March 2026  
Last reviewed: 11<sup>th</sup> March 2026  
Next review due: 11<sup>th</sup> March 2027

**Version: 1.1**

