PRIVACY POLICY

POLICY

1. OVERVIEW

This privacy policy explains how The Cause Collective (TCC) collects, stores, uses, and shares **personal information**. Personal information means information about an identifiable individual (Privacy Act 2020, section 7). The Privacy Commissioner provides guidance on sensitive personal information under the Privacy Act 2020.[1]

This policy applies to all personal information collected, stored, used, and shared by TCC. Coverage is universal: the policy protects everyone whose personal information TCC holds, including people who are not Māori or Pacific. This policy is subordinate to the Data Management Policy. In case of conflict, the Data Management Policy prevails.

2. SCOPE

In the event of overlap, the hierarchy of policies is:

1. **Data Management Policy** (governing)
2. **Privacy Policy** (personal-data compliance)
3. **Cybersecurity Policy** (technical incident management)
4. **IT Security Policy** (infrastructure and access control)
5. **AI Policy** (automated-tool use).

We recognize the value of people's lived experiences as a legitimate source of information and a key contributor to our work. We collect, store, use, and share personal information to carry out our functions and activities. All data and information we collect are considered *taonga* and treated with the utmost respect. We will protect it and ensure that it is managed appropriately.

TCC collects personal information about the people it employs, works with and serves, both directly from them and from the organisations it works with.

TCC's obligations around managing and using personal information are governed by the Privacy Act 2020.

[1] Refer to Office of the Privacy Commissioner at https://www.privacy.org.nz/

Policy Name:	Privacy Policy	**Date Issued:**	August 2021
Policy Number:	INFPL12	**Date Updated:**	October 2026
Version:	2026/04	**Date Approved:**	October 2026
Approved By:	The Cause Collective Board of Trustees	**Next Review Date:**	October 2027

TCC will only collect, use, and share personal information where there is a lawful purpose connected with its functions and activities, and only to the extent necessary to fulfil that purpose.

3. PRIVACY OFFICER

TCC's Privacy Officer is the Digital Transformation Lead. The Chief Financial Officer is the second Privacy Officer and acts when the Digital Transformation Lead is unavailable. They are responsible for:

- Monitoring compliance with this policy
- Directing activities that ensures all relevant people are familiarised with this policy and have access to ongoing access to training and resources
- Dealing with requests made to TCC for personal information
- Liaising with the Privacy Commissioner or other statutory bodies when required.

In the absence of a nominated Privacy Officer at any time, the above responsibilities will default to TCC Chief Executive.

The Privacy Officers are contactable at: privacy@thecausecollective.org.nz

4. DATA MINIMISATION AND SUPPRESSION

Where personal information is used, the number and accuracy of data points should be limited as much as reasonably possible (for example, age group rather than date of birth), depending on the use case.

Access to personal information follows this same principle and is discussed in the IT Security policy.

When reporting to funders or making data publicly available, care must be taken to ensure no data point can be composed of fewer than six records to avoid reidentification.[2]

5. MANAGING A PRIVACY INCIDENT

TCC will align responses to privacy incidents with best practice advice from the Office of the Privacy Commissioner.[3]

---

[2] As utilised by Statistics New Zealand in governing IDI output. Please see: https://www.stats.govt.nz/assets/Uploads/Integrated-data-infrastructure/microdata-output-guide-fourth-edition.pdf

[3] https://www.privacy.org.nz/responsibilities/privacy-breaches/

Anyone identifying a potential privacy breach must notify a Privacy Officer as soon as possible. A response will then be implemented encompassing the following tasks:

- Containing the incident.
- Notification to cybersecurity insurers, where applicable.
- Evaluate risks.
- Notification to affected persons.
- For a breach that has caused, or is likely to cause, serious harm, the Privacy Commissioner and affected people are notified as soon as practicable, as the Privacy Act 2020 requires. TCC works to the Privacy Commissioner's expectation of notifying the Commissioner within 72 hours.

The Chief Executive decides whether a breach is notified, on the advice of a Privacy Officer. The steps are set out in TCC's Managing a Privacy Breach procedure.

6. PRIVACY PRINCIPLES

TCC adheres to the 14 information privacy principles in the Privacy Act 2020:

- **Purpose of Collection:**
  - Personal information of staff and contractors is collected for payroll and HR purposes.
  - Whānau and patient information is collected to deliver TCC's own services and to meet its reporting requirements.
- **Source of Information:** Obtain information directly from the individual when possible.
- **Transparency:**
  - TCC staff and contractors providing personal information for payroll or HR purposes should note this policy and have its provisions explained during orientation.
- **Notification of indirect collection:** when TCC collects personal information about a person from someone else, it takes reasonable steps so the person knows it has, why, who will receive it, how to contact TCC, and their access and correction rights, unless the Act exempts it.
- **Fair Collection:** Avoid using unfair or intrusive means to collect information.
- **Storage and Security:** Protect information from unauthorized access or misuse.
- **Access:** Individuals have the right to access their personal information.
  - To request access email us at privacy@thecausecollective.org.nz
- **Correction:** Individuals can request corrections to their information.
  - To correct your personal information, email us at privacy@thecausecollective.org.nz
- **Accuracy:** Ensure information is accurate before use.

- **Retention:** Retention and secure deletion processes are governed by the Data Management Policy (see Section: Data Security).
- **Use:** Use information only for its collected purpose.
- **Disclosure:** Disclose information only for its collected purpose.
- **Disclosure outside New Zealand:** personal information is only sent to an organisation outside New Zealand where it will be protected by safeguards comparable to New Zealand's, or with the person's authorisation. Any decision to store or share data outside New Zealand goes to the AI, Data, Privacy, and Digital Transformation Group first for assessment and recommendation, and to the Chief Executive for approval (see the Data Management Policy, sections Jurisdiction and Data Sharing).
- **Unique Identifiers:** Use unique identifiers only when necessary.

For more details, visit the website of the NZ Privacy Commissioner:
https://www.privacy.org.nz/

7. COLLECTION OF PERSONAL INFORMATION

We collect personal information directly from individuals when they take part in TCC's services, and during safety checks, human resource management and research activities.

Types of Personal Information Collected

- Full name, date of birth, gender, ethnicity
- Contact details: addresses, email, phone numbers
- Qualifications and employment details
- Police vetting details and outcomes
- Experiences related to our services
- Questions or comments submitted on our social platforms
- Responses to surveys, research, interviews, or focus groups

We may also collect information from the organisations we work with to deliver our services, and from third parties for investigating issues and complaints.

Where personal information reflects cultural, spiritual, or community identity, TCC will apply additional care consistent with Māori and Pacific data-sovereignty principles. This additional care sits alongside the policy's universal coverage and does not narrow who the policy protects.

8. COOKIES

We use cookies to understand how people engage with our website, help users navigate efficiently, perform site functions, and gather usage information.

Cookies are also used for features like keeping you logged in while navigating the site. You can opt out by changing your browser settings.

9. WEBSITE ANALYTICS

We use Google Analytics to collect data about your website interactions to improve your experience. This data is aggregated and non-identifiable. You can opt out by changing your browser settings or visiting the Google Analytics opt-out page: https://tools.google.com/dlpage/gaoptout

Other websites and social media services may have their own privacy policies and tracking mechanisms.

10. SURVEYS, NEWSLETTERS AND COMMUNITY CONTRIBUTIONS

When participating in our social media forums, your name will be displayed. We recommend not posting personal information like email addresses, home addresses, or phone numbers.

From time to time we may use third-party providers to gather business information (for example surveys). These providers have their own privacy policies which should be reviewed before supplying identifying information.

11. HOW WE USE PERSONAL INFORMATION

Personal information is used to carry out our functions and may be disclosed to entities like NZ Police for vetting. **Uses Include**

- **Operational Functions**: Conducting statutory and administrative tasks of TCC, such as Payroll or HR.

Use of personal information in AI tools follows the AI Policy (INFPL14).

12. DISCLOSURE OF PERSONAL INFORMATION

Personal information may be disclosed to:

- **New Zealand Police:** For obtaining a police vet.
- **External Agencies:** To prevent harm or uphold the law.

We adhere to the Privacy Act's limits on using and disclosing personal information.

13. COMPLAINTS

To file a complaint about a privacy breach or harm, contact us at the following email address: privacy@thecausecollective.org.nz

The process is as follows:

- **Acknowledgment:** Within two working days.
- **Response:** Our Privacy Officer will respond within 20 working days.
- **Escalation:** If unsatisfied, write to the Chief Executive within 30 days.

External Complaint: You may also contact the Privacy Commissioner: www.privacy.org.nz/your-rights/making-a-complaint/#contact

14. PERSONAL ACCOUNTABILITY

All TCC personnel, and members of the Board of Trustees, are personally accountable for safeguarding personal information. Accountability means accepting that the buck stops with you. Responsibility means exercising due care to maximise positive outcomes and minimise harm.

Any violation of this policy will be deemed serious misconduct under the Staff Code of Conduct and may result in disciplinary action or termination (see Staff Code of Conduct: Serious Misconduct section).

Governance and role responsibilities are defined in the Data Management Policy (section: Data Governance and Roles).

15. POLICY REVIEW AND UPDATES

This Privacy Policy was approved by the Board of Trustees on 21 October 2026 and will be reviewed annually or earlier to ensure its continued relevance and compliance with applicable laws and regulations. Any updates or revisions to this Policy will be

communicated to relevant stakeholders. The AI, Data, Privacy, and Digital Transformation Group reviews this policy and endorses it before it goes to the Board for approval.

16. ASSOCIATED DOCUMENTS

- Data Management Policy
- IT Security Policy
- Cybersecurity Policy
- AI Policy
- AI, Data, Privacy, and Digital Transformation Group – Terms of Reference
- Managing a Privacy Breach procedure (version 4, April 2026)
- Request for Personal Information procedure (version 1, April 2026)
- Privacy Risk Assessment Checklist
- TCC Privacy Statement
- Staff Code of Conduct
- Complaints Policy
- New Zealand Privacy Act 2020
- New Zealand Privacy Amendment Act 2025 (principle 3A, in force 1 May 2026)
- Health Information Privacy Code 2020