Coromandel Independent Living Trust
TE ROOPUU WHAIORA

3.6 Privacy Policy

Links to CILT Values

- Kaitiakitanga- Our Responsibilities
- Whakawhanaungatanga - Respectful Relationships
- Manaakitanga - Care for all people

Policy Rational:
All persons have the right to have their privacy respected. Coromandel Independent Living Trust (CILT) must promote and protect individual privacy.
The safety of the Trustees, staff, contractors, volunteers and clients of CILT, including children, young people, the disabled, the elderly and the disadvantaged, is paramount.

Policy Purpose:
To provide guidelines for procedures associated with personal information.
To clarify the expected performance/practice standards for CILT staff, Trustees, contractors, volunteers & clients.

Application:
This policy applies to CILT Trustees, staff, volunteers, contractors, clients and service participants..

Guiding Principles:

Principle 1 - Purpose for collection of personal information
CILT must only collect personal information if it is for a lawful purpose connected with the organisation functions and activities, and the information must be necessary for that purpose.
If the personal information you are asking for isn't necessary to achieve something closely linked to CILT's activities, you shouldn't collect it.

Principle 2 - Source of personal information - collect it from the individual
Personal information should be collected directly from the person it is about.

Principle 3 - Collection of information from subject - what to tell the individual
CILT should be open about why personal information is being collected and what they will do with it.
When CILT collects personal information, it must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if the information isn't provided.

Principle 4 - Manner of collection
Personal information must be collected in a way that is lawful and seen as fair and reasonable in the circumstances.
You need to take particular care when collecting information from children and young people.

- Except where concerns of abuse or neglect are held, an individual's permission **must** be sought before information is collected &/or shared.
- Where photographs are to be used in the public domain, where ever possible, permission is sought from those depicted in the photographs, before they are used.
- All written permission agreements for collecting and sharing personal information, refer to the Privacy Act (2020), and require the individual's signature.
- The Application Form completed by all employment applicants, informs applicants that their signature gives permission for CILT to contact their listed referees.
- Intake procedures exist for confirming attendance in all programmes.
- All CILT staff, contractors, Trustees and volunteers are required to sign, and adhere to CILT's Code of Ethics, which refers to the Privacy Act (2020), as a condition of maintaining their employment relationship with CILT.

Principle 5 - Storage and security of information
CILT must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information.

- All paper-based information held regarding any individual is held in a locked filing cabinet.
- All electronically stored information must be password protected.
- Only the staff collecting the information and staff who require the information for the functions and activities for which it was collected should have access to the information
- Staff individual files are also available to both the General Manager and the Human Resources Coordinator.

Principle 6 - Access to personal information
People have a right to ask for access to their own personal information.
People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person, unless you are acting on that person's behalf and have written permission.

- Where a service participant has High Needs, their delegated whanau/family member as specified on the participants privacy document may have access to the participant's Individual File.

Principle 7 - Correction of personal information
A person has a right to ask the organisation to correct information about them if they think it is wrong.
If the organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and CILT should take reasonable steps to do so.

Principle 8 - Accuracy of personal information
CILT must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.

Principle 9 - Retention of personal information
The organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used.

- Where a Trustee, staff member, contractor, volunteer or service participant ceases their employment/ relationship with CILT, personal information is kept for seven years, then paper records are destroyed by shredding, and all online personnel records are deleted.
- Employ wages and time records, and holiday and leave records must be kept for 6 years.
- The formal records of a trust (agendas and minutes and formal reports to the trustees etc) must be kept for the lifetime of the trust [per the Trusts Act]
- financial records must be kept for 7 years [per IRD requirements]
- Curriculum Vitae (CV) belonging to unsuccessful employment applicants are deleted once they have been informed of the outcome or in the case of paper based applications returned (where a stamped, self-addressed envelope is provided by the applicant) or shredded.

Principle 10 - Limits on use of personal information
The organisation can only use personal information for the purpose it was collected unless the person in question gives their permission for their information to be used in a different way.

- If there is another piece of legislation which says that personal information must, shall, or must not be used in a certain way, this will override the general provisions of the Privacy Act.

Principle 11 - Disclosure of personal information
The organisation must only disclose personal information for the purpose for which it was originally collected or obtained unless:

- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

3.6.1 Responding to a potential breach of privacy

Where CILT becomes aware of a breach of privacy, there will be an immediate investigation and response as quickly as possible, including contact within 48 hours of the reporting breach of privacy, and response in writing within 14 days. This will help minimise any harm caused to the affected people and CILT.

There are five key steps in dealing with a privacy breach:

⇒ Step one: acknowledge the complaint

⇒ Step two: listen to complainant

⇒ Step three: investigate the issues the complainant raised

⇒ Step four: try to resolve the issue

⇒ Step five: rebuild the relationship

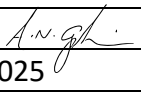
CILT will follow the above steps in line with the Office of the Privacy Commissioner's guidance for dealing with a breach of privacy, found here:
https://www.privacy.org.nz/responsibilities/handling-privacy-complaints-a-step-by-step-guide/

Under the Privacy Act 2020, where the privacy breach has caused or is likely to cause anyone serious harm, CILT must notify the Privacy Commissioner and any affected people as soon as practicable after becoming aware that a notifiable privacy breach has occurred.
In this instance, the breach notification will be made to the Office of the Privacy Commissioner no later than 72 hours after CILT is made aware of a notifiable privacy breach.

Following a privacy breach, the General Manager will arrange a meeting with the parties responsible for the project in which the breach occurred, and assess how the breach occurred, the impact of the breach, and develop a process for ensuring the breach does not occur again.

Legislative Compliance Considerations

- Privacy Act 2020
- Trusts Act 2019

Policy Reviewed by the Trust Board	Signed: 
Date Approved:	28 May 2025
Next Review Date:	May 2028
Revokes Policy Reviewed:	19/08/2021