

Privacy Statement

Auckland Coastguard Incorporated

Control Table	Detail
Document	Privacy Statement (public and member facing)
Owner	General Manager, Auckland Coastguard Inc.
Version	2.0
Effective from	October 2025
Next review	October 2027
Companion document	ACI Privacy Policy (internal)

1. About this statement

Auckland Coastguard Incorporated ("Auckland Coastguard", "we", "us", "our") is an incorporated society and a registered charity. We are a volunteer marine search and rescue organisation operating on the Hauraki Gulf and surrounding waters.

This statement explains what personal information we collect about you, why we collect it, what we do with it, and the rights you have over it. It applies to our volunteer members, our employees and contractors, our supporters and donors, people we assist, participants in our education programmes, and visitors to our premises and our website.

We handle personal information in accordance with the Privacy Act 2020 and, where health information is involved, the Health Information Privacy Code 2020.

This statement sits alongside our internal Privacy Policy, which sets out how our people are required to handle personal information. This statement tells you what we do. The policy tells our people what they must do.

2. The information we collect

The information we hold varies depending on your relationship with us. The categories below describe what we may collect. We do not collect all of it about every person.

2.1 Volunteer members, employees and contractors

- Identity and contact details, including name, date of birth, postal and physical address, email address and phone numbers.
- Next of kin and emergency contact details.

- Demographic information such as gender, where you choose to provide it, which helps us understand and improve the diversity of our crew.
- Membership records, including your unit, role, joining date, subscription status and service history where available.
- Availability, attendance and deployment records, including the taskings, duties and events you have been assigned to.
- Training, assessment and competency records, including course attendance, endorsements and qualifications.
- Certificates, tickets and licences, including maritime qualifications where provided, first aid certificates and driver licence details where a role requires them.
- Health and medical information relevant to your role, including medical fitness declarations, injury and incident records, allergies and any accommodations you need.
- Police vetting results.
- Human resources records, including applications, references, performance and development discussions, disciplinary matters and complaints.
- Bank account details, where we reimburse expenses or pay wages, and tax and payroll information for employees.
- Photographs and video of you taken at training, at events and during operations.
- Records of your use of our systems, including sign in logs and activity records.

2.2 People we assist

- Information provided to us, or to our rescue agency partners and regulators like the Rescue Coordination Centre when you request or receive assistance, including your name, contact details, vessel details and location.
- Information about the incident, including what happened, the assistance we provided, and observations recorded by our crew.
- Health information where we provide first aid or where your condition is relevant to the response.
- Photographs, video and audio captured during an operation, including radio recordings, vessel systems data and imagery used for navigation, situational awareness and later review.

2.3 Education and community programme participants (youth)

- We do not hold the information of participants under the age of 16, as all interaction with community groups with are all completed with the attending group responsible for their attendance and adult to minor ratios.
- We record the Group Name, and primary contact responsible's name, and numbers attended to any event we host.
- We collect and share photographs and video, only where a parent or caregiver and the Community Group Leader have given consent.

Where a programme is delivered under a Coastguard New Zealand national framework, such as Safe Boating, information may also be collected and held by Coastguard New Zealand. Their privacy statement applies to information they hold.

2.4 Supporters, donors and members of the public

- Name and contact details.
- Donation and fundraising history, and gift preferences.
- Records of your correspondence and interactions with us.
- Marketing preferences, and whether you have opted in or out of our communications.

We do not store, process or handle your credit or debit card numbers. Card payments are processed by our payment providers, currently ASB and Stripe, who hold the industry certifications required to handle card data securely.

2.5 Visitors to our premises

- CCTV footage, described further in section 5.
- Visitor sign in records and access control records.

3. How we collect information

We collect information directly from you wherever we reasonably can, for example when you apply to join, complete a form, attend training, make a donation or contact us.

Sometimes we collect information about you from other people or organisations, because collecting it from you directly is not possible or would undermine the purpose of collection. This includes agencies and sources like the Rescue Coordination Centre New Zealand and other emergency services when we are tasked to an incident, Coastguard New Zealand as our national body, referees you nominate, New Zealand Police when we carry out vetting, and a parent or caregiver where the person concerned is a child.

We will always tell you why we are collecting your information, what we will do with it, who will hold it, and whether providing it is optional or required, unless an exception in the Privacy Act applies. We will never collect information by unfair, unlawful or unreasonably intrusive means.

4. Why we collect and use information

We use personal information for the purpose it was collected for and for closely related purposes. In practice that means:

- Carrying out search and rescue operations and other assistance on the water.
- Managing volunteer membership, deployment, crew engagement and safety.
- Maintaining our employee records
- Delivering, recording and assuring training, assessment and competency.
- Meeting our obligations as an employer and as a person conducting a business or undertaking under the Health and Safety at Work Act 2015.
- Running our education and community programmes.
- Fundraising, donor care and communicating with our supporters.
- Managing our premises, assets and security.
- Meeting our legal, regulatory and reporting obligations.

- Reviewing and improving how we operate, including operational debriefs and service improvement.
- Producing statistics, reports and research. Wherever possible this information is aggregated or anonymised so individuals cannot be identified.

We will not use your information for an unrelated purpose unless you have authorised it, the information is publicly available, the use is necessary to prevent or lessen a serious threat to public health or safety or to the life or health of any person, or an exception in the Privacy Act applies.

Before we use or disclose your information, we take reasonable steps to check that it is accurate, up to date, complete, relevant and not misleading.

5. CCTV

We operate CCTV cameras at our premises. We use the footage to keep people safe, to protect our vessels, buildings and equipment, and to review incidents that occur on site or on our rescue vessels.

- Clear signage is displayed so that people know CCTV is operating before they enter a monitored area.
- Access to footage is limited to a small number of authorised people and is granted on a least privilege basis.
- Every viewing, extraction and disclosure of footage is logged.
- Footage is automatically overwritten on a routine cycle, unless it has been retained for an investigation, a legal proceeding or a regulatory request.
- We do not use CCTV to monitor the routine performance of members or staff.

6. Our membership register

As an incorporated society we are required by the Incorporated Societies Act 2022 to keep a register of members, which includes each member's name, contact details and the date they became a member. Our constitution sets out how members may access the register and on what conditions.

If you are elected or appointed as an officer of the society, some of your details are provided to the Registrar of Incorporated Societies and appear on the public Incorporated Societies Register.

This is a legal requirement of membership and of holding office, and it applies regardless of any other preference you have set with us.

7. Sharing your information

We do not sell, rent or trade personal information.

We share information where it is necessary for the purpose it was collected for, where you have authorised it, or where the law requires or allows it. The main situations are set out below.

7.1 Emergency response and operations

During and after an incident we share information with the Coastguard New Zealand, Rescue Coordination Centre New Zealand, New Zealand Police, Hato Hone St John and other ambulance services, Fire and Emergency New Zealand, harbourmasters, hospitals and other rescue units if they are involved or if we are required to do so by law, so that the response can be coordinated and continued.

7.2 Coastguard New Zealand

As a Coastguard unit we share membership, training, operational and incident information with Coastguard New Zealand for national coordination, training records, insurance, national reporting and support services.

7.3 Regulators, investigations and the courts

As a first responder organisation we are required to provide information, which may include incident records, employment and training records, health and safety records and CCTV footage, to bodies including, but not limited to:

- Maritime New Zealand, for maritime incident reporting and safety investigations.
- WorkSafe New Zealand, for notifiable events and investigations under the Health and Safety at Work Act 2015.
- The Coroner and New Zealand Police, for death investigations, formal incident reporting and emergency management.
- The Transport Accident Investigation Commission, courts and tribunals, where required.

7.4 Service providers

We share information with organisations that provide services to us, such as software platforms, payment processors, insurers, auditors, banks and professional advisers. They may use the information only to provide the service to us, and they are required to protect it to the same extent or better than we are.

7.5 Serious threats

We may disclose information without your authorisation where it is necessary to prevent or lessen a serious threat to public health or safety, or to the life or health of any person.

8. The systems we use, and information held overseas

Like most organisations, we rely on third party software and cloud services to operate. We use them for the following purposes:

What we use systems for	The kind of information involved
Membership, crew management and engagement, event management, deployment, training and competency administration	Contact details, next of kin, availability, service history, qualifications
Operational and incident information	Incident records, tasking information, information about people we assist, operational imagery

What we use systems for	The kind of information involved
Health, medical fitness and vetting records	Medical fitness declarations, injury records, vetting decisions
Supporter and donor relationships, and the communications we send	Contact details, donation history, communication history, marketing preferences
Finance, payroll and payment processing	Bank account details, payroll and tax information, donation records
Email, messaging, documents and collaboration	Whatever is contained in the correspondence and documents themselves
Premises security	CCTV footage, access control and visitor records
Youth and community programmes	As disclosed above in 2.3

We do not name individual products in this statement, because the tools we use change as the organisation grows and continue to make the commitment to improve digitally. What does not change is the standard we hold them to. Before we adopt any system that will hold personal information, we assess its security, its contractual terms, where it stores information, and what happens to that information if we stop using it. A system that cannot meet our minimum standard is not used.

We keep a register of every system we use, where it is stored and who is accountable for it. You are welcome to ask our Privacy Officer for the current details at any time, and we will tell you.

Information held in these systems remains under our control. Our providers hold and process it for us and on our instructions under contract, and they are not permitted to use it for their own purposes.

Some providers store information on servers outside New Zealand, commonly in Australia, Singapore the United States or Europe. Where we disclose personal information to an overseas person or organisation that is not acting as our agent, we first satisfy ourselves that comparable privacy safeguards apply, or we obtain your authorisation.

9. Keeping your information safe

- We encrypt information in transit and at rest where possible.
- We require multi factor authentication on our core systems where this capability exists.
- We limit access to those who need it for their role, and we remove access promptly when a role or membership ends.
- We keep software patched and up to date.
- Our staff complete privacy and information handling training and our volunteers are kept informed of their obligations.
- We assess the privacy and security of a new platform before we adopt it.

No system can be guaranteed completely secure, but we take these obligations seriously and we review our controls regularly.

10. How long we keep information

We keep personal information only for as long as we need it for the purpose it was collected for, or for as long as the law requires. Some records must be kept for long periods, for example health and safety records, incident records and records relating to exposure to hazards.

Our retention periods are set out in the retention schedule in our internal Privacy Policy. You may ask our Privacy Officer how long we will hold a particular type of record.

When information is no longer required, we securely destroy or de-identify it.

11. Your rights

11.1 Access

You can ask us whether we hold personal information about you, and ask for a copy of it. That includes asking whether you appear in our CCTV footage.

11.2 Correction

You can ask us to correct information you believe is wrong, incomplete or out of date. If we do not agree to make the correction, you can ask us to attach a statement of the correction you sought, and we will do so.

11.3 How to make a request

Contact our Privacy Officer using the details in section 13. We may ask you to confirm your identity before we release information. We will respond as soon as we can and no later than 20 working days after we receive your request. If we need more time, we will tell you within that period and explain why.

There are limited grounds in the Privacy Act on which we may withhold information, for example where releasing it would unreasonably affect another person's privacy, or where it consists of evaluative material given in confidence. If we withhold information we will tell you why, and tell you that you can complain to the Office of the Privacy Commissioner.

11.4 Marketing choices

If you receive newsletters, appeals or other marketing from us, every message includes an unsubscribe option. You can also ask us to stop at any time by contacting us directly. We will still send you messages we need to send you, such as operational, membership and safety communications.

12. If something goes wrong

If we have a privacy breach that is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and the people affected as soon as practicable, as required by the Privacy Act 2020.

If you think your information has been mishandled, please tell our Privacy Officer. We would rather hear about it early.

13. Contact us

	Detail
Privacy Officer	General Manager
Email	privacy@aci.org.nz
Postal Address	3 Solent Street, Mechanics Bay, Auckland 1010

If you are not satisfied with how we have responded, you can complain to the Office of the Privacy Commissioner. Visit www.privacy.org.nz, phone 0800 803 909, or email enquiries@privacy.org.nz.

14. Changes to this statement

We review this statement at least every two years, and whenever we make a significant change to the way we handle personal information. The current version is always available on our website and on request. The version and effective date are shown at the top of this document.