New Zealand Clay Target Association

Data Governance Policy

Last Updated June 2026

Introduction

The NZCTA uses data for operational activities, regulatory compliance, and service delivery and is committed to managing this data correctly and securely. This Data Governance Policy establishes a framework for the management, use, and protection of NZCTA's organisational data to ensure its quality, integrity, security, accessibility, and appropriate use across the Organisation.

1. Purpose and Definition

This policy establishes how The New Zealand Clay Target Assn Inc. (referred to herein as "the Organisation") collects, manages, stores, disposes of, shares, and protects personal information and data in accordance with New Zealand law. It ensures that personal, organisational, and sporting data is used responsibly, transparently, and securely to support the goals of the organisation while protecting the rights of individuals.

"Data" means any recorded information, regardless of format or medium, that is created, collected, stored, processed, transmitted, or used by the Organisation in support of its activities. This includes the personal information of individuals, structured and unstructured data, metadata, documents, records, databases, files, messages, images, audio, and other digital or physical information assets.

2. Scope

This policy applies to:

- All NZCTA Employees, Volunteers and Council members.
- All personal data, including member, and sponsor/supplier information.
- Organisational data, including financial, operational, and performance data.
- Digital and physical data systems managed by the Organisation.

3. Legal Framework

This policy is guided by:

- Privacy Act 2020 – governs collection, use, and disclosure of personal information.
- Unsolicited Electronic Messages Act 2007 ("UEMA") – regulates commercial electronic communications.
- Harmful Digital Communications Act 2015 – addresses online harassment and harmful content.

4. Principles of Data Governance

The Organisation will manage data in line with the following principles:

- Accountability – Data is managed under the oversight of the Executive Officer in line with legal and ethical standards.
- Transparency – Individuals will be informed about how their data is collected, used, stored, and shared.
- Lawfulness & Fairness – Data will only be collected and used for legitimate purposes related to sporting operations.
- Data Minimisation – Only the information necessary for operations will be collected.
- Accuracy – Data will be kept up to date and corrected when errors are identified.
- Storage Limitation – Data will not be kept longer than required by law or operational need.
- Security – Appropriate technical and organisational safeguards will protect data from loss, misuse, unauthorised access, or disclosure.

- Rights of Individuals – Individuals can access and correct their data under the Privacy Act 2020.

5. Data Categories and Management

- Personal Information includes names, contact details, participation history, event results, and financial membership status. Consent to collect and obtain personal information of any entity or person will be obtained where required, except where the information is already publicly available (e.g., Incorporated Society Requirements to hold details of officers of member clubs).
- Sponsor/Supplier information includes names, contact details, agreements or contracts, financial contributions, bank account details, invoices and payment records,
- Operational and Sporting Data includes personal information, competition entries, competition results, and team selection information.
- Communications Data such as Email, SMS, and app communications must comply with the Unsolicited Electronic Messages Act 2007 (UEMA). Marketing communications from third party suppliers connecting with NZCTA clubs or individual members require explicit opt-in consent.
- Informational messages sent by the Organisation to individual shooter members and Club members, which are exempt from the UEMA rules, relate to the normal functioning of the Organisation. These informational messages include:
    - Registration confirmations for an event.
    - Sending out a member magazine detailing results, upcoming events, or annual general meeting notices.
    - Messages to a team confirming team place and event information.
    - Communications regarding a member's ongoing membership, account, subscription or payments made to the member.

6. Data Security and Access

Access to data is role-based and restricted to authorised individuals only. The Organisation’s membership information is maintained by the Executive Officer in a password-protected system, while physical files are stored securely with restricted access. All data breaches must be reported immediately to the Executive Officer, and serious breaches must be notified to the Office of the Privacy Commissioner (OPC) as required by the Privacy Act 2020.

7. Data Sharing and Third Parties

The Organisation may share data with trusted third-party service providers where necessary for operations, including:

- Payment processing by financial institutions
- IT and cloud service providers
- Competition and event management systems
- Communication platforms (magazine, Facebook, newspapers)

All third-party providers must:

- Use the information only for authorised purposes
- Implement appropriate security safeguards
- Comply with applicable privacy laws

Any contract with third-party providers will contain a clause advising of the requirement for them to safeguard all information provided to them during the term of engagement.

8. Retention and Disposal

Membership and participation data will be retained for 10 years following the last recorded activity, while NZCTA financial records will be kept for a minimum of 7 years in accordance with IRD requirements. When data is no longer required, it will be securely deleted or destroyed.

9. Roles and Responsibilities

- The NZCTA Council approves this policy and oversees compliance.
- The Executive Officer ensures compliance with the Privacy Act 2020, manages access/correction requests, and reports breaches.
- All employees and volunteers (including Clubs and their Office Staff) must ensure compliance with the Privacy Act when handling data and report all breaches to NZCTA.
- Members/Participants are responsible for providing accurate information and advising of changes.

10. Training and Awareness

All Council members will be advised on data protection and privacy obligations when appointed to the Council, and any updates to the Data Governance policy communicated.

11. Breach Management

Any suspected or actual privacy breach must be reported immediately to the Executive Officer or the NZCTA President and a post-incident review conducted to ensure the breach is not repeated. Policies will be updated where necessary following major incidents and serious breaches that are likely to cause harm will be notified to the OPC and affected individuals as required. Corrective measures will be implemented in all cases to prevent recurrence.

12. Policy Review

This policy will be reviewed at least every two years, or earlier if legislation or operational needs change.