


PISTOL CLUB

PRIVACY POLICY

Member, Participant and Governance Information

Document owner	Public Officer/Secretary
Policy administrator	Club Secretary / appointed Privacy Officer
Version	1.1 — July 2026
Approval status	APPROVED AND CURRENT - REVIEW/UPDATE SCHEDULED (NOT FOR WITHDRAWAL)
Review cycle	At least every two years, and earlier following material legal, system or affiliation change
Classification	CLUB IN CONFIDENCE — CONTROLLED DOCUMENT

DOCUMENT CONTROL This controlled document must not be duplicated, reproduced or distributed, in whole or part, without Club authorisation. This restriction does not prevent the Club from publishing or providing its privacy policy or privacy notices, giving members access, obtaining professional advice, reporting to an affiliated body or regulator, or making any disclosure required or authorised by law.

Policy statement

Newtec Pistol Club Incorporated (Club) respects privacy and will handle personal information lawfully, fairly, transparently and securely. The Club adopts the Australian Privacy Principles (APPs) as its minimum privacy standard, whether or not every APP is legally mandatory for the Club in a particular circumstance.

1. Purpose and application

This policy explains how the Club collects, holds, uses, discloses, secures, accesses, corrects and disposes of personal information. It applies to Committee members, office bearers, employees (if any), volunteers, coaches, range officers, selectors, officials, contractors and any person handling information for the Club.

It covers information about members, applicants, prospective members, visitors, competitors, athletes, officials, volunteers, parents and guardians, complainants, respondents, witnesses, contractors, donors, sponsors and website or social-media users.

LEGAL POSITION The Privacy Act 1988 (Cth) generally applies to organisations with annual turnover above \$3 million and to some smaller organisations regardless of turnover. The Club voluntarily applies the APPs as a governance baseline. Where legislation, a court order, NSW firearms requirements, child-safety obligations, the Club constitution, or a binding affiliated-body rule imposes a higher or inconsistent requirement, the Club will follow the applicable law or binding requirement and document the basis.

2. Governing framework

This policy is informed by and should be read consistently with:

- Privacy Act 1988 (Cth), including the 13 Australian Privacy Principles and, where applicable, Part IIIC (Notifiable Data Breaches scheme);
- Privacy and Other Legislation Amendment Act 2024 (Cth), including applicable commencement dates for later reforms;
- Spam Act 2003 (Cth) and Do Not Call Register Act 2006 (Cth) for electronic and telephone communications;
- NSW firearms, child-safety, incorporated-association, record-keeping and other laws relevant to Club operations;
- Shooting Australia Privacy Policy and applicable integrity/member-protection policies;
- NSW Amateur Pistol Association (NSWAPA) constitution, code of conduct and disciplinary policy; and
- Sport Integrity Australia's National Integrity Framework and privacy requirements where they apply.

This policy does not replace a specific collection notice, consent form, integrity policy, competition condition, employment record obligation or statutory requirement. Those instruments operate together; the more privacy-protective applicable requirement should be used unless prohibited by law.

3. Key definitions

Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or recorded in material form.
Sensitive information	Includes health information, criminal record information, racial or ethnic origin, religious beliefs, sexual orientation and membership of certain associations, where covered by law.
Health information	Information or an opinion about an individual's health, disability or health service, including emergency and participation-related information.
Data breach	Loss, unauthorised access, unauthorised disclosure, alteration or misuse of personal information.
Affiliated bodies	Bodies through which the Club or its members participate, including NSWAPA, Target Pistol Australia/Pistol Australia, Shooting Australia and Sport Integrity Australia, as applicable.



4. Privacy governance and accountability

The Committee is accountable for privacy governance. It must ensure proportionate practices, procedures and systems, approve material changes, oversee serious incidents and resource reasonable security controls.

- The Secretary is the Privacy Officer unless the Committee appoints another person in writing.
- Access is role-based and limited to people who need the information for authorised Club duties.
- Committee members and volunteers must preserve confidentiality during and after their appointment and return or securely delete Club records when their role ends.
- Privacy and information-security risks must be considered before new forms, databases, cloud services, cameras, apps, mailing tools, AI tools or data-sharing arrangements are introduced.
- Material privacy decisions, disclosures, incidents, complaints, access refusals and destruction actions must be documented.
- The Club will maintain a data inventory and periodically review access permissions, retention and third-party providers.

5. Information the Club may collect

The Club only collects information reasonably necessary for its functions and activities and will use data minimisation. Depending on the relationship, this may include:

- identity and contact details, date of birth, signature, emergency contacts and parent/guardian details;
- membership category, membership history, financial status, affiliation/capitation identifiers, qualifications and volunteer roles;
- firearms licence or permit type, number, status and expiry date, and sighting/verification records where required; copies are not retained unless reasonably necessary and authorised;
- attendance, sign-in, competition entries, scores, classifications, selection, training, accreditation and participation records;
- payments, invoices, refunds and limited transaction records (the Club does not retain full payment-card security codes);
- health, disability, accessibility, medication or emergency information voluntarily provided or reasonably required for safe participation;
- complaints, incident reports, disciplinary matters, witness material, integrity reports and outcomes;
- working-with-children or other screening status where required, without retaining more identity documentation than necessary;
- photographs, video, livestreams, CCTV, audio, website enquiries, email and social-media interactions; and
- technical information such as IP address, device/browser data, security logs and cookies where used by Club systems.

FIREARMS-SENSITIVE INFORMATION Firearms licence, attendance and participation information may create heightened personal-safety and security risk. It must never be published in a member directory, social-media post, public results list or general email group. Access and disclosure require a clear authorised purpose.

6. How information is collected and notice

Where reasonable and practicable, information is collected directly from the individual through membership and renewal forms, visitor registers, competition systems, consent forms, incident reports, email, telephone, the website and in person. Information may also come from a parent or guardian, referee, affiliated body, coach, official, service provider, publicly available source, police or regulator where lawful.

At or before collection—or as soon as practicable—the Club will provide a concise privacy notice stating the Club's identity and contact method, what is collected, why, the usual disclosures, consequences of not providing it, how to access or correct it, how to complain, and any likely overseas disclosure. Sensitive information will generally be collected with express, informed, voluntary, current and specific consent unless an exception applies.



People may interact anonymously or under a pseudonym where lawful and practicable. Identification is required where necessary for membership, firearms compliance, insurance, competition eligibility, safeguarding, payments, access control, incident management or legal obligations.

7. Children and young people

- Collect only the minimum information needed for participation, safety, consent, affiliation and safeguarding.
- Use age-appropriate explanations and obtain parent/guardian consent where the young person cannot validly consent or where policy/law requires it.
- Do not publish a child's full name with address, school, contact details, licence/permit details or other identifying security information.
- Obtain specific image/publicity consent and respect withdrawal for future use, subject to lawful archival and competition records.
- Restrict complaint, health and child-safety information to authorised personnel and approved reporting channels.

8. Purposes of use

The Club may use information for the primary purpose notified at collection, including:

- assessing and administering membership, renewals, fees, voting eligibility and member communications;
- verifying licences, permits, age, qualifications, financial status, affiliations and lawful range access;
- operating ranges, events, competitions, training, coaching, teams, awards and volunteer rosters;
- meeting safety, emergency, insurance, child-safety, integrity, disciplinary, governance and legal obligations;
- capitation, affiliation, accreditation, grading, entry, results, selection and reporting to relevant sporting bodies;
- managing incidents, complaints, investigations, appeals, disputes and procedural fairness;
- maintaining facilities, security, access control, business continuity and fraud prevention;
- providing requested services, responding to enquiries, improving Club operations and keeping historical records; and
- promoting Club activities using images, results or stories only where authorised and appropriately minimised.

A secondary use requires consent unless it is within reasonable expectations and related to the primary purpose (directly related for sensitive information), or is otherwise required or authorised by law. Personal information must not be entered into public generative-AI tools or unapproved platforms.

9. Disclosure and information sharing

The Club may disclose the minimum necessary information to:

- NSWAPA, Target Pistol Australia/Pistol Australia, Shooting Australia, Sport Integrity Australia, competition organisers and accreditation or selection bodies;
- NSW Police, Firearms Registry, emergency services, child-protection authorities, courts, tribunals, regulators or other authorities where required or authorised;
- insurers, brokers, auditors, accountants, legal advisers and professional investigators;
- approved technology, payment, website, communications, storage and document-destruction providers bound by appropriate safeguards;
- officials, coaches, range officers and volunteers who need the information for an authorised function; and
- other persons with the individual's consent or where a permitted legal situation applies.

Integrity and disciplinary information must be shared on a strict need-to-know basis, with procedural fairness and confidentiality. Participants must not retaliate against a person for making a lawful privacy, safety or integrity report.



10. Overseas disclosure and cloud services

Some approved providers or affiliated sporting systems may store or process information outside Australia. Before disclosure, the Club will make reasonable enquiries about data location, security, contractual safeguards and privacy protections; provide notice where required; and take reasonable steps required by APP 8. Countries may vary by provider and must be identified in the relevant collection notice where practicable. The Privacy Officer maintains the current provider register.

11. Communications, website, images and CCTV

Operational membership messages are sent where reasonably necessary. Marketing or promotional electronic messages must identify the Club, include a functional unsubscribe method and comply with applicable consent and spam requirements. Unsubscribing from promotions does not prevent essential safety, governance, membership or legal communications.

- Use blind-copy, an approved mailing platform or individual delivery for group emails; do not expose recipient lists without authority.
- Website analytics and cookies must be limited, documented and configured to minimise collection; third-party tracking requires review.
- Photography and video must avoid displaying licence details, sign-in books, addresses, security controls or firearm-storage information.
- Competition results may be published where reasonably expected or notified, using only necessary identifiers and classifications.
- CCTV, if used, is for safety, security and incident investigation. Signage must be displayed, access restricted, and audio recording disabled unless specifically lawful and approved.
- Members and visitors must not record or publish another person's personal information in a manner inconsistent with Club rules, consent or safety.

12. Data quality, access and correction

The Club takes reasonable steps to keep information accurate, complete, relevant and up to date. Individuals should promptly notify the Secretary of changes to contact, emergency, licence/permit, affiliation or eligibility details.

A person may request access to or correction of their personal information through the Secretary/Privacy Officer. Identity will be verified proportionately. The Club will respond within a reasonable period and generally without charge, except reasonable access costs where lawful. Access may be refused or limited only on a lawful ground—for example where it would unreasonably affect another person's privacy, prejudice an investigation, reveal evaluative material in a protected process, create a serious safety risk, or be unlawful. Reasons and available complaint avenues will be provided where required.

13. Security and handling rules

- Use unique accounts, strong passwords and multi-factor authentication where available; never share credentials.
- Store paper records in locked facilities; do not leave sign-in books, applications or incident files unattended.
- Encrypt or otherwise protect portable devices and sensitive files; minimise downloads and removable-media use.
- Send sensitive information only through approved channels, verify recipients, and avoid ordinary group email attachments.
- Do not keep Club records solely in personal email, personal cloud drives or messaging apps; transfer them promptly to the approved record system.
- Apply role-based permissions, timely access removal, backups, updates, malware protection and secure disposal.
- Report loss, misdirection, suspicious access, phishing or unauthorised disclosure immediately to the Privacy Officer.
- Do not discuss membership, complaint, health, licence or disciplinary information in public or with people without an authorised need to know.

CLUB IN CONFIDENCE — CONTROLLED COPY

No unauthorised duplication, reproduction or distribution. Authorised access and legal disclosure remain permitted.



14. Retention and secure disposal

The Club keeps information only for as long as reasonably required for the purpose collected, legal and insurance obligations, dispute limitation periods, archival value and affiliated-body requirements. The Committee must approve a retention schedule. Until adopted, the following controls apply:

- review active member data at renewal and archive former-member records with restricted access;
- keep financial, governance, attendance, competition, safety and incident records for the applicable statutory, insurance or affiliation period;
- keep complaint and disciplinary records long enough to implement outcomes, manage appeals and meet safeguarding, integrity, insurance and legal needs;
- retain CCTV only for a short, documented period unless preserved for an incident or legal purpose;
- delete duplicate working copies and securely shred paper or securely erase electronic media when no longer required; and
- where lawful and practicable, de-identify information retained for statistics, historical analysis or service improvement.

LEGAL HOLD No record subject to an investigation, complaint, insurance claim, subpoena, regulator request, anticipated litigation or other legal hold may be destroyed until the hold is formally released.

15. Data breaches and incident response

Anyone who suspects a data breach must immediately contain the issue where safe, preserve evidence and notify the Privacy Officer. They must not conceal the incident, contact affected people independently, or make public statements unless authorised.

Contain: stop further access or disclosure without destroying evidence; recover misdirected material where possible.

Assess: identify what happened, whose information is affected, sensitivity, likely consequences and available remediation.

Escalate: notify the President and Committee-designated incident lead; obtain legal, insurer, cyber or affiliated-body advice where appropriate.

Remediate: reset credentials, remove access, correct processes, support affected people and document actions.

Notify: where the NDB scheme applies, assess suspected eligible breaches promptly and complete the statutory assessment within the required period; notify the OAIC and affected individuals when required. Other legal, insurer, police, child-safety or affiliation notices may also apply.

Review: record lessons, control improvements, owners and completion dates.

16. Privacy enquiries and complaints

Privacy enquiries, access/correction requests and complaints should be addressed to the Club Secretary / Privacy Officer through the official contact details published on the Club website or delivered to the Secretary at the clubhouse. Mark correspondence “Private and Confidential — Privacy Officer”.

A complaint should identify the conduct, dates, information involved, desired outcome and relevant evidence. The Club will acknowledge it promptly, manage conflicts of interest, investigate fairly, protect confidentiality as far as possible, provide a written outcome and explain any review option. The Club aims to respond within 30 days; complex matters may take longer with progress updates.

If the Privacy Act applies and the person is dissatisfied, they may complain to the Office of the Australian Information Commissioner. Integrity, child-safety, police or affiliated-body reporting options remain available and are not displaced by this procedure.



17. Breaches of this policy

Unauthorised access, use, disclosure, copying, retention, destruction or concealment of personal information may result in removal of access, corrective directions, volunteer or employment action, Club disciplinary action, notification to an affiliated body, insurer, regulator or police, and other lawful action. Outcomes must follow the constitution, applicable policies and procedural fairness.

18. Review, approval and publication

The Committee reviews this policy at least every two years and sooner after a material incident, legal reform, affiliation change, new technology, significant data-sharing arrangement or regulator guidance. The version history must record approvals and substantive amendments.

The Club will make an appropriate current privacy policy or public-facing privacy notice available free of charge where required by APP 1. A controlled internal version may include operational details that are not suitable for public release. From 10 December 2026, the Club must also assess whether any computer program uses personal information to make decisions that could reasonably be expected to significantly affect an individual's rights or interests, and update disclosures if APP 1.7–1.9 apply.

Approval record

Committee resolution	July Meeting 26
Approval date	24/06/2026
Effective date	24/07/2026
Next review due	01/10/2027
President signature	Bruce Bourke
Secretary signature	Mark Web

Version history

Version	Date	Approved by	Summary
1.0	July 2026	Committee	Initial comprehensive policy

Authoritative references (current at July 2026)

- **Privacy Act 1988 (Cth) and Australian Privacy Principles** — <https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act>
- **OAIC — Australian Privacy Principles Guidelines (updated 13 May 2026)** — <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>
- **OAIC — Notifiable Data Breaches scheme guidance** — <https://www.oaic.gov.au/privacy/notifiable-data-breaches>
- **OAIC — Small business coverage guidance** — <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business>
- **Shooting Australia — Privacy Policy (version 2.2, 19 July 2024)** — <https://shootingaustralia.org/privacy-policy/>
- **NSWAPA — Constitution and governance resources** — <https://www.nswapa.org.au/>
- **NSWAPA — Disciplinary Policy (adopted 26 October 2024)** — <https://www.nswapa.org.au/DisciplinaryPolicyOct2024.pdf>
- **Sport Integrity Australia — Privacy** — <https://www.sportintegrity.gov.au/privacy>

CLUB IN CONFIDENCE — CONTROLLED COPY

No unauthorised duplication, reproduction or distribution. Authorised access and legal disclosure remain permitted.



AUTHORITATIVE DOCUMENT CONTROL RECORD

Document reference	NPC-PRV-POL-001
Adopted	24/06/2026
Enacted / effective	24/07/2026
Minute reference	july26meeting
Owner	Public Officer/Secretary
Next review	01/10/2027
Status	APPROVED AND CURRENT - REVIEW/UPDATE SCHEDULED (NOT FOR WITHDRAWAL)

Control note: This authoritative record replaces all earlier non-current control labels in this file. The document is approved and current, and is scheduled for review and updating, not withdrawal.



AUTHORITATIVE DOCUMENT CONTROL RECORD

Document reference	NPC-PRV-POL-001
Adopted	24/06/2026
Enacted / effective	24/07/2026
Minute reference	july26meeting
Owner	Public Officer/Secretary
Next review	01/10/2027
Status	APPROVED AND CURRENT - REVIEW/UPDATE SCHEDULED (NOT FOR WITHDRAWAL)

Control note: This authoritative record replaces all earlier non-current control labels in this file. The document is approved and current, and is scheduled for review and updating, not withdrawal.



AUTHORITATIVE DOCUMENT CONTROL RECORD

Document reference	NPC-PRV-POL-001
Adopted	24/06/2026
Enacted / effective	24/07/2026
Minute reference	july26meeting
Owner	Public Officer/Secretary
Next review	01/10/2027
Status	APPROVED AND CURRENT - REVIEW/UPDATE SCHEDULED (NOT FOR WITHDRAWAL)

Control note: This authoritative record replaces all earlier non-current control labels in this file. The document is approved and current, and is scheduled for review and updating, not withdrawal.

Approved amendment — document control

Field	Draft entry
Document reference	NPC-PRV-POL-001
Version	v1.1
Status	APPROVED AND CURRENT — REVIEW/UPDATE SCHEDULED
Approved	24/07/2026
Owner	Public Officer / Secretary unless the Committee determines otherwise
Approval / effective / minute	24/07/2026 24July26meeting
Amendment purpose	Adds proportionate information-security and data-breach controls to the Privacy Policy.

Appendix — Information security and data-breach response

A. Classification and access

Class	Examples	Control
Public	Approved publications	Integrity and version control
Internal	Routine procedures	Authorised users and controlled storage
Confidential	Finances, approvals, security, investigations	Need-to-know, MFA, restricted sharing
Personal/sensitive	Membership, health, complaints, WWCC	Minimum collection, role-based access, secure transmission
Highly restricted	Junior, identity and firearms/security details	Named custodians, encryption and access review

B. Baseline controls

- Unique accounts, strong passphrases and multi-factor authentication
- Quarterly access review and immediate removal on role departure
- Protected backup with tested restoration
- Supported, patched and encrypted devices
- No sensitive information in informal group chats
- Approved retention and secure disposal

C. Breach response

- Contain without destroying evidence; disable compromised access and preserve logs.
- Assess affected systems, people, information, recipients and continuing harm.
- Escalate immediately to the Secretary/Public Officer and an unconflicted committee contact.
- Assess notifications to affected people, OAIC/NDB scheme if applicable, Police, Registry, OCG, bank, insurer and providers.
- Recover trusted systems, monitor misuse and document root cause and closure.