

Prima Nota Inc. – Data Management & Privacy Policy

Adopted: 08.12.2025

Applies to: All committee members, facilitators, contractors, and volunteers who handle or access organisational information or participant data.

1. Purpose

Prima Nota Inc. values transparency, trust, and the privacy of all individuals involved in our programs.

This policy explains how we collect, store, use, and protect personal and organisational data in accordance with the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) and best practices for small incorporated associations.

2. Scope

This policy applies to:

- Personal information collected from members, volunteers, participants, donors, sponsors, and partners.
 - Organisational data such as meeting records, project documentation, grant applications, photos, and media.
 - Any electronic or physical storage system used for Prima Nota's administrative or program purposes.
-

3. Types of Information Collected

- Contact details (name, phone, email, address)
 - Demographic information (age group, language, cultural background — if voluntarily provided)
 - Photographs, video, and audio recordings (with consent)
 - Membership and attendance forms
 - Volunteer and contractor details (including Working With Children Check status)
 - Financial records related to sponsorships, grants, or reimbursements
-

4. How Data is Collected

Data may be collected through:

- Membership, volunteer, or event registration forms
- Online tools such as Google Forms, spreadsheets, or email
- Written consent forms for photography, video, and media publication
- Direct communication (email, phone, or in person)

All data is collected only for organisational purposes — never for personal or unrelated use.

5. How Data is Used

Collected data may be used to:

- Communicate with members and volunteers

- Manage programs, workshops, and events
- Apply for grants and report outcomes to funding bodies
- Promote activities (with consent for public photos or quotes)
- Meet legal, insurance, or child-safety requirements

Prima Nota Inc. does not sell, rent, or trade personal information under any circumstances.

6. Data Storage and Security

- Digital data is stored in secure cloud services (Google Workspace, encrypted drives, or equivalent).
 - Paper records are kept in locked filing cabinets or secure home offices accessible only to authorised committee members.
 - Access to member data is restricted to those who need it for legitimate organisational tasks.
 - All reasonable steps are taken to protect data from loss, unauthorised access, modification, or disclosure.
-

7. Sharing and Disclosure

Information may be shared only when:

- Required by law (e.g., insurance or grant audits).
- Explicit consent has been obtained (e.g., photo releases).

- It is necessary to deliver a program in partnership with another organisation (and that partner has equivalent privacy standards).

All sharing of personal information must be approved by the Chairperson or Secretary.

8. Data Retention and Disposal

- Records are retained only as long as needed for operational, legal, or historical purposes.
 - Outdated digital files are permanently deleted from cloud storage.
 - Paper documents are securely shredded when no longer required.
 - Financial records are kept for at least seven (7) years as required by the Associations Incorporation Act 1985 (SA).
-

9. Access and Correction

Individuals have the right to:

- Request access to the personal information held about them;
- Request corrections if that information is inaccurate or outdated.

Requests should be made in writing to the Secretary, who will respond within a reasonable timeframe.

10. Breach Response

In the event of a suspected or actual data breach:

1. The Chairperson and Secretary must be notified immediately.
2. The committee will assess the impact and take steps to contain and rectify the breach.
3. If required, affected individuals and relevant authorities will be informed promptly.

11. Review

This policy will be reviewed every two years, or sooner if required by law or operational change, to ensure continued compliance with the Australian Privacy Principles and evolving best practice for community organisations.