

Australian Voice Association

Data Security Policy

Version 1.0 | March 2026

1. Purpose

This policy sets out how the Australian Voice Association (AVA) collects, stores, uses, and protects personal and sensitive information. It applies to all committee members, volunteers, and anyone who handles AVA data on behalf of the organisation.

AVA is committed to handling information responsibly and in line with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs).

2. What Information We Hold

AVA may collect and store the following types of information:

- Member contact details — names, email addresses, phone numbers, and postal addresses
- Financial and payment information — records related to membership fees, event payments, or invoices
- Event registration details — attendance records, dietary requirements, and participation history
- Abstracts and research submissions — academic work submitted for conferences or publications

3. How We Collect Information

Information is collected directly from members and participants through membership forms, event registrations, email correspondence, and abstract submission processes. AVA will not collect more information than is reasonably necessary for its activities.

4. Email Inbox Security

The AVA email inbox is a key point of contact for members and the public. The following practices apply:

- The inbox is managed by a single designated person (the Inbox Manager)
- Access is protected by a strong, unique password
- The password must not be shared with unauthorised individuals
- The Inbox Manager is responsible for handling all incoming correspondence securely and confidentially
- If the Inbox Manager role changes, the inbox password must be updated immediately
- Emails containing sensitive member information should not be forwarded to personal email accounts

5. Data Storage and Access

AVA takes the following steps to keep stored data secure:

- Member and financial records are stored in password-protected files or platforms
- Access to sensitive data is limited to those who need it to carry out AVA activities
- Physical documents containing personal information are stored securely and disposed of appropriately when no longer needed
- Cloud storage or shared drives used for AVA data must require login and not be publicly accessible

6. Use of Information

Personal information collected by AVA will only be used for the purpose it was collected. This includes:

- Communicating with members about membership, events, and AVA activities
- Processing payments and maintaining financial records
- Managing event registrations and logistics
- Reviewing and publishing conference abstracts and research (with consent)

AVA will not sell, rent, or share member information with third parties for commercial purposes.

7. Data Breach Response

If AVA becomes aware of an actual or suspected data breach (e.g. unauthorised access to the inbox, lost device, or accidental disclosure), the following steps should be taken:

- Contain the breach as quickly as possible (e.g. change the affected password immediately)
- Notify the AVA President or relevant committee member
- Assess the likelihood and severity of harm to affected individuals
- If the breach is likely to cause serious harm, notify affected individuals and consider reporting to the Office of the Australian Information Commissioner (OAIC)

8. Member Rights

Members have the right to:

- Request access to the personal information AVA holds about them
- Request corrections to any inaccurate information
- Ask for their information to be deleted, where reasonable and permitted

Requests can be made by contacting the AVA inbox. AVA will respond within a reasonable timeframe.

9. Policy Review

This policy will be reviewed annually, or sooner if there are significant changes to AVA's operations or relevant legislation.

10. Contact

For questions about this policy or how your information is handled, please contact AVA via the official email inbox.