



Privacy

1. Introduction

Anglican Overseas Aid (AOA) is committed to protecting the privacy of the information provided to AOA by all supporters and stakeholders. We recognise our duty to protect personal information from misuse and to disseminate only information that is necessary for our work and respectful of dignity and privacy.

2. Purpose and Scope of the policy

- To ensure that AOA's communication, marketing and fundraising operations and materials comply with Australian privacy legislation.
- To ensure AOA provides accountable and transparent privacy compliance.
- To explain why and how we protect, collect, use, disclose and store personal information.

3. Application

This Privacy Policy applies to Board members, staff, contractors and volunteers of AOA. From here on, these groups will be collectively referred to in this policy as 'AOA People'. The Policy also applies to information we hold about partners, supporters and prospective supporters visiting AOA programs.

4. International and National Frameworks

This policy is informed by the following:

- Australian Council for International Development (ACFID) Code of Conduct
- DFAT - Australian NGO Cooperation Program (ANCP) Accreditation Framework
- Australian Privacy Principles, established under the Privacy Act 1988 (Cth).

5. Guiding Principles

- AOA People adhere to the organisation-wide requirements for the protection of privacy.
- All information obtained and stored is done in alignment with Australia's privacy legislation requirements.

6. Implementation

6.1 Collecting and Holding of Personal Information

- AOA collects and stores only those personal details relevant to its work.
- The personal information we collect may include supporter reference number, name, date of birth, address, telephone and/or mobile number, email address, evidence of identity and tax file number (for employment purposes), bank account or credit card details, company information, records of donations, payment information for those donations, and any communications.
- We may also collect and hold sensitive information such as church affiliation, working with children and criminal background checks for AOA people e.g. supporters or Board members visiting our partners overseas. Sensitive information about an individual will only be collected when they consent to its collection and/or when the information is necessary for our work or required by Australian law.

6.2 How we Collect and Hold Personal Information

- **AOA will collect information that is shared directly with us via fair and lawful methods**, including but not limited to correspondence, website access, electronic sign-up, surveys, donations, job applications, and conversations that occur in the course of our work.
- **Visiting our website**, we may use cookie and tracking technology. These technologies gather information about the page(s) users visit and how they interact with those page(s). They can allow visitors to customise the page(s). They do not collect personal information but may link to information previously supplied and be personally identifiable.
- AOA's website(s) and social media sites may contain links to third-party websites whose operators may or may not be governed by Australian legislation, the Australian Privacy Principles, or adhere to a privacy policy. We have no control over, and are not responsible for, third parties' privacy policies and practices. Supporters who engage with AOA through thirdparty social media platforms like Facebook are subject to that platform's privacy terms and conditions.
- We may also collect information available in the **public domain** and from **social media platforms** such as X (formerly Twitter), Meta (Facebook, Instagram), TikTok or LinkedIn. These organisations will explain how they handle your data in their privacy policies.
- We may collect personal information from **third parties** where users have agreed to support AOA and have given consent for their details to be shared in this way. This may include recruitment service providers, former employers, law enforcement agencies and other government entities. For example, if a supporter visits one of our partners overseas, we will conduct checks for child protection.
- We may also collect information about employees throughout their employment with AOA. This may include remuneration and salary information, start and end dates, working days and hours, details of promotions, performance information, attendance and absence data, training records, details related to the use of company property

and equipment (including emails and software), and information related to disciplinary or grievance investigations.

- You may choose not to provide us with your personal information, for example, if you give anonymously. In this case, we could not provide you with tax-deductible or other receipts.

6.3 Collecting Biometric Information

- Anglican Overseas Aid may use and store biometric information through a third party digital asset management system. Where using and storing biometric Anglican Overseas Aid will:
 - Enable the feature lawfully to make sure that using facial recognition is permitted in every jurisdiction where individuals depicted in the digital assets are located.
 - Obtain valid consent (such as in a release form) before collecting or uploading any individual's Biometric Information to the Service.
 - Provide notice to ensure each individual is told that their Biometric Information will be used for automated tagging inside HIVO and may be processed by AWS in Australia.
 - Respect data-subject rights to use the Service's search and deletion tools to comply with any access, correction, deletion or objection requests relating to Biometric Information.
 - Configure the appropriate permissions to restrict and limit the number of users that can enable or access the Facial-Recognition Feature and set retention rules that meet privacy and records-management policies and obligations.
- This information may be used to:
 - detect faces in still images and video frames stored
 - convert each face into an encrypted mathematical facial vector that cannot be reverse-engineered to recreate the original image; and
 - Attach a person's name or subject tags to the relevant asset to improve searchability, reduce manual tagging effort, assist in tracking media consent and release forms and have the ability to respond to Data-Subject access or erasure requests.
- Anglican Overseas Aid remains the data controller.

6.4 Protecting information

AOA takes all reasonable steps to protect all personal information from unauthorised access, misuse, loss and disclosure. Only authorised employees, agents, and contractors (who have agreed to keep information secure and confidential) have access to this personal information. Information is stored within our CRM, email database, employee portal, accounting system, project management tool, and intranet filing system, which maintains a high level of security, including two-factor authentication for users and timed session logout to prevent unauthorised access.

6.5 The purposes for which personal information is collected, held, used and disclosed

Personal details are used to:

- Process donations and issue receipts.
- Provide regular supporter contact and support for fundraising purposes.
- Establish, manage and maintain supporter, employee and other stakeholder relationships
- Support marketing functions e.g. employee name, bio, image and job title on AOA's website or in other marketing materials

If an individual does not want AOA to use their information for any of the above purposes, they may notify AOA at aoa@anglicanoverseasaid.org.au or 1800 249 880.

Our data handling principles include:

- Collecting only the information needed for our work
- De-identifying or anonymising data where appropriate
- Retaining data as necessary, in line with legal and operational requirements
- Secure disposal or deletion of information when it is no longer required

If we use personal information in ways other than as stated in this policy, we will ensure we comply with Privacy legislation.

We may disclose an individual's personal information to:

- AOA people for purposes necessary for our work
- Trusted third parties such as bank processing, database storage and maintenance, and mailing houses for purposes necessary for our work. Occasionally, AOA may undertake joint initiatives with Anglican or like-minded organisations, which necessitate the use of supporter details through a third-party mailing house
- Travel agents and suppliers of accommodation and travel services for employee travel
- Superannuation funds
- The Australian Taxation Office or another governmental authority as required by law.

Mailing lists of supporters or other contacts are never sold, rented or exchanged to third parties.

Where we use third-party service providers (such as payment processors, CRM providers, or IT support), we ensure they meet our privacy and security expectations. Contracts include confidentiality and data protection clauses, and we only share information necessary for them to perform their function.

6.6 Accessing personal information and keeping details accurate and up-to-date

Whilst AOA keeps personal information secure from others, individuals may request access to their information at any time. Individuals who want to know what information AOA holds about them, or who would like to correct an error, should contact the Privacy Officer on 1800 249 880 or (03) 9495 6100 or aoa@anglicanoverseasaid.org.au. When an individual requests access to their information, AOA may ask for identity verification. AOA will only provide information to the individual concerned or another person they have authorised, such as a legal guardian or authorised agent.

Personal information held by AOA regarding employees is subject to the “employee records exemption” under the Privacy Act and does not have to be disclosed on request. Other persons, such as job applicants, can request copies of their personal information by contacting the Privacy Officer.

AOA is committed to keeping details up-to-date after being informed of any change of details. Supporters have the right to:

- Access their personal information stored by AOA, subject to exceptions allowed by law
- Have their names deleted from mailing lists, including those that AOA may intend to use
- in joint initiatives
- Be informed about whether those seeking donations are volunteers or paid staff
- Be informed about the causes for which funds are being raised
- Gain information on the application of their donation
- Identify collectors who will hold documentation confirming their affiliation with AOA.

6.7 Risk Management

Privacy risk is managed in accordance with AOA’s FA 18 Risk Management policy.

Projects or business activities that involve handling personal information will systematically assess the impact that the project or business activity might have on the privacy of individuals in the design stage and at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction and de-identification. If any personal information will be collected, stored, used or disclosed in the project or business activity, a privacy impact assessment may be conducted using the [OAIC Privacy Impact Assessment Tool](#).

6.8 Training

All staff and volunteers who handle personal information receive regular privacy and cybersecurity training and are required to adhere to strict confidentiality obligations.

6.9 Eligible Data Breaches

The Privacy Act stipulates reporting and management requirements for certain data breaches, known as ‘eligible data breaches’. An ‘eligible data breach’ occurs when personal information held by AOA is lost, or unauthorised access, disclosure, or other interference has taken place, and the access or disclosure would likely result in serious harm to the individuals to whom the information relates. ‘Serious harm’ may include physical, emotional, economic, and financial harm, as well as reputational damage.

Examples of a data breach include:

- A device containing personal information of staff or supporters is lost or stolen;
- One of AOA’s databases containing personal information is hacked;
- AOA mistakenly provides personal information to the wrong person.

AOA have procedures to detect, respond to, and report any data breaches in line with the Australian Notifiable Data Breaches (NDB) scheme. If AOA suspects there has been an eligible data breach, AOA must carry out an assessment within 30 days of the suspicion to determine whether a data breach has occurred. In the case of an eligible data breach, AOA must take all steps to immediately contain the breach and determine who needs to be notified of the breach (whether internally and/or externally), what the best form of notification is, and how this process will be managed.

7. Complaints or Concerns

Respecting your privacy is very important to us, and we make every effort to ensure this occurs. However, if you believe we have breached your privacy rights in any way or you would like to discuss any concerns, please get in touch with us at complaints@anglicanoverseasaid.org.au

8. Definitions

- **Collection:** includes gathering, acquiring or obtaining personal information from any source and by any means, including from individuals, other entities, generally available publications (e.g. Church contact lists), information associated with web browsing, such as personal information collected by cookies. Collection may also take place when personal information is generated from other data held by AOA (e.g. a customer mailing list)
- **Explicit Consent** is given when an individual actively agrees — by ticking a box, signing a form, or giving verbal confirmation — to a specific, clearly stated use of their data.
- **Implied Consent** is inferred from the context when the individual provides information because it is obviously required for the interaction.
- **The Privacy Act 1988** (Cth) (Privacy Act) is an Australian law that regulates the handling of personal information about individuals.
- **Personal information** is information or an opinion about an identified individual or an individual who is reasonably identifiable.
- **Sensitive Information** is a subset of personal information and is defined as:

- information or an opinion (that is also personal information) about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, or criminal record
- health information about an individual
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates

9. Review

This policy and related procedures will be reviewed no later than October 2028.