Privacy Policy

Policy Statement

At Transform Aid International Ltd ("TAI"), every supporter, volunteer, church, partner organisation and child partner are important to us.

TAI respects and safeguards your privacy and confidentiality. We are committed to accountability and transparency. We continue to strive for the highest possible standards as we comply with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APP).

We are committed to protecting our staff, supporters and volunteers. Without them we would not be able to continue caring for and empowering our partner organisations as they seek to lift themselves and their communities out of poverty. TAI recognises that giving to an organisation is a very personal decision. We recognise that you place your trust in us through your dealings with us and we will do everything we can to maintain that confidence.

We are committed to protecting the privacy of our stakeholders in partner organisations, including child partners. We recognise our duty to protect personal information from misuse, to only disseminate information that is necessary for our work and is respectful of dignity and privacy.

Scope

This policy applies to all TAI representatives including staff, volunteers, contractors and suppliers who preform services on our behalf, whether in Australia or overseas.

Aspects of this policy apply additionally to third parties including: implementing Partners, project participants, supporters of TAI and its subsidiaries, and participants in events or trips facilitated by TAI or its subsidiaries.

Policy Objectives

The objectives of this policy are to:

- Explain why and how we protect, collect, use, disclose and store personal information.
- Ensure that TAI maintains internal practices, procedures and systems that are compliant with the APPs.

What does the policy look like in practice?

The kind of personal information we collect and hold

TAI only collects personal information about you that is necessary for our work. Personal information is defined as any information that can be used to identify you. If the information that we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

The personal information we collect may typically include your name, address, telephone number, email address, date of birth, occupation, marital status, records of your donation/s and payment information for those donation/s, and any communications you have with us.

We may also collect and hold sensitive information such as church affiliation, working with children and criminal background checks for supporters travelling to visit 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.

We may also collect information about employees throughout their employment with TAI. This may include remuneration and salary information, start and end dates, working days and hours, details of promotions, performance information, attendances and absences, training records, details related to the use of TAI property and equipment (including emails and software), and information related to disciplinary or grievance investigations.

How we collect and hold personal information

Shared directly with us

TAI will collect this information via lawful and fair methods including but not limited to correspondence, website access, electronic sign-up, surveys, donations, event entry forms and conversations between you and our representatives.

When you visit our website

We use "cookies" to track visits to our website. Our cookies do not collect personal information and can be disabled at any point through your internet browser settings. Find out more about cookies by reading our Website Rules.

We may use scripts and third party cookies to collect information about your interactions with our website to help us learn more about how supporters use our site and to help us advertise. The information collected is stored securely. TAI also allows tracking pixels on our Baptist World Aid website from companies like Google Analytics, Meta and Microsoft to help us learn more about how people engage with our content and advertising efforts..

Publicly available data

We may also collect information that is 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.

Indirectly from third parties

We may collect personal information from third parties where you have agreed to support TAI and given your consent for your details to be shared in this way. This may include law enforcement agencies and other government entities, for example if you are attending a supporter trip overseas, we will conduct checks for child protection purposes.

For organisations such as schools or churches we may also gather information from your public website, such as size, contact details, and values.

You may choose not to provide us with your personal information, for example, if you give anonymously. In this case we would not be able to provide you with tax deductible or other receipts, or access to protected areas of our website.

Protecting your information

We are committed to protecting the personal information you entrust to us. We take this responsibility seriously and apply a range of safeguards to keep your data secure.

We implement industry-standard security measures to protect your information from misuse, loss, unauthorised access, modification, or disclosure. These include:

- Securing our physical premises and IT systems
- Using password-protected access and Multi-factor authentication (MFA)
- Secure cloud-based data storage with encryption
- Firewalls and intrusion detection systems
- Regular software updates and vulnerability patching
- Endpoint protection and device management
- Monitoring and auditing our systems for security vulnerabilities

We make all reasonable efforts to ensure that your information is stored securely, via our secure password and firewall-protected servers, both in electronic and physical forms, and that only those persons who require access are authorised. We use role-based access controls to ensure data is only available to authorised personnel. Staff are employed on the basis that they will protect information about you. All donations and communications made via our website are secure. All electronic financial transactions and payment details entered through our website or by staff directly into our database are protected by encryption technology.

We will keep a record of your personal information for as long as you continue to engage with us unless you advise differently. If we no longer need your information or you ask us to delete your personal information, we will delete or de-identify the information in accordance with our Record Retention Policy. In some instances, we are required to maintain your records by law, or for audit or risk management purposes. For example, if you have donated to TAI and received a receipt for taxation purposes, by law we must keep a record of your details for seven years.

How We Protect Children and Youth

If you are 18 or older, we will normally assume that you can make your own privacy decisions. When you are under 18, we may need to confirm your decision with a parent or guardian.

We also expect you to take particular care with the images of children from our programs, as we do. We request that you respect the consent given by parents or community leaders by not copying these images unless we provide specific permission. Please refer to our Website Rules for guidance on how you may use images from our website and our Child Safe Policy & Code of Behaviour for further guidance on use of child images generally.

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

The information we collect is used to:

- Process donations, commitments and sponsorships
- Issue receipts and donation statements
- Respond to your comments or questions
- Provide you with access to protected areas of our website
- Provide follow up information about the work of TAI

- Provide selected information about child partners (sponsored children) to their sponsors
- Seek your continued support
- Offer other programs or opportunities that may be of interest to you
- Research your attitudes and understanding of TAI and our programs, or about aid and development
- Report internally
- Deal with enquiries and complaints made by you
- Provide third parties with statistical information about our supporters (but those third parties will not be able to identify any individual supporter from information provided to them)
- Establish, manage and maintain employee relationships

If you do not wish TAI to use your information for any of the purposes listed above, please notify us on 1300 789 991.

We follow best-practice data handling principles, including:

- Collecting only the information needed for our work
- De-identifying or anonymising data where appropriate
- Retaining data only for as long 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 the requirements of Privacy law.

We may disclose your personal information:

a) To our employees, related bodies corporate (for example, our wholly owned subsidiary, Baptist World Aid Australia), contractors or service providers for purposes necessary for our work.

b) To our contractors who perform tasks directly on our behalf (for example, mail houses, which send our marketing communications, or research agencies). These contractors may also collect personal information on our behalf. We require them to sign strict privacy and security agreements, and they are also bound by the Australian Privacy Principles. These agreements ensure that these contractors keep your personal information confidential and do not use it for any purpose other than the work we have contracted them to perform.

c) To reputable cloud-based organisations with robust security protocols to store your data securely including but not limited to Microsoft Azure, Amazon Web Services (AWS), Oracle – NetSuite and Cisco, 8x8. The secure storage facilities/data centres for these organisations are often located overseas.

d) To the extent that we are required by law to do so;

e) In connection with any ongoing or prospective legal proceedings;

f) To establish, exercise or defend our legal rights (including providing information to others only to the extent required for the purposes of fraud prevention, managing cases of suspected or substantiated fraud, reducing credit risk and as otherwise required);

g) To any person who we reasonably believe may apply to a court or other competent authority for disclosure of that personal information, where in our

reasonable opinion, such court or authority would be reasonably likely to order disclosure of that personal information.

We do not pass on personal information to any third parties other than those stated in this policy or publish them in our publications or on our website without explicit supporter permission. We do not buy or sell personal information from or 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.

How you can access your personal information and seek its correction

Whilst we keep all personal information about you secure from others, you may request access to your information at any time. If you would like to know what information we hold about you, or there is an error you would like to correct, please contact our Privacy Officer. We may ask for verification of your identity when you request access to your information. TAI will only provide information to you or another person you have authorised, such as a legal guardian or authorised agent.

TAI may decline to provide details of personal information to a supporter in any legal dispute where access is not permitted.

There may be cases where we cannot provide access to personal information we hold, for example, where providing access would interfere with the privacy of others or breach confidentiality. We will not disclose addresses of child partners to supporters or any other information that would enable a supporter to identify the child's private home (see our Child Safe Policy). If we refuse to grant access to personal information, we will provide written reasons for the refusal.

Personal information held by TAI 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.

Updating Information

TAI aims to ensure that the information we collect about you is accurate, complete and up to date. We may at times contact you to ensure that it is.

Please let us know if the personal information that we hold about you needs to be corrected, updated or completed.

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 contact our Privacy Officer

The Privacy Officer
Transform Aid International
Locked Bag 2200
NORTH RYDE BC NSW 1670

Email: privacy@baptistworldaid.org.au
Phone: 1300 789 991

Where you request a response, you can expect to hear from us within 30 days. We will treat your complaint or request with confidentiality.

Governance and Risk Management

The Risk and Compliance Committee (RCC), including the Privacy Officer as a committee member, provides oversight of organisation risk and compliance matters and provides regular reports to the Board. Privacy risk is a key organisational risk and is managed in accordance with the Organisation Risk Management Framework.

Projects or business activities that involves the handling of 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 will be conducted using the OAIC Privacy Impact Assessment Tool.

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 TAI 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: -

1. A device containing personal information of clients is lost or stolen;
2. One of TAI's databases containing personal information is hacked;
3. TAI mistakenly provides personal information to the wrong person.

We have procedures in place to detect, respond to, and report any data breaches in line with the Australian Notifiable Data Breaches (NDB) scheme. If TAI suspects there has been an eligible data breach, TAI must carry out an assessment within 30 days of the suspicion to determine whether a data breach has occurred. The Crisis Management Team is responsible for determining if an eligible data breach has occurred. In the case of an eligible data breach, TAI must take all steps to immediately contain the breach, 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.

For details on the procedure of handling an eligible data breach, please refer to the Business Continuity Policy, Crisis Management Plan, and Notifiable Data Breaches Procedure.

Third Party Websites

For marketing purposes, we may upload customer lists (with email addresses, or phone numbers) to third party websites/tools so that we can communicate with supporters through those

platforms. We do this by adding pixels to our website. This could include Meta, Adroll, Spotify and/or Google.

Our website includes hyperlinks to, and details of, third party websites. We have no control over, and are not responsible for, the privacy policies and practices of third parties.

Responsibilities

Position/ Delegated Body	Responsible for
Director Governance, Risk and Business Optimisation	• Strategic oversight of this policy
Privacy Officer	• Responding to enquiries or requests for privacy related information
Risk and Compliance Committee	• Operational oversight of organisation risk and compliance matters • Preparation of regular reports to the Board.
Crisis Management Team	• Investigation and management of any data breach

Compliance with this policy will be monitored by the positions listed in the table above. Noncompliance with this policy will be managed in accordance with the Disciplinary Policy.

Accessing the Policy

This policy will be available on TAI's SharePoint and from our websites.

Training

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

Review and Amendment

This policy will be reviewed triennially or sooner as required, and amendments will be made as required in response to changing circumstances. Any changes will be updated on our website.

Definitions[1]

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 tale place when personal information is generated from other data held by TAI (e.g. a customer mailing list)

[1] Definitions informed by the app-guidelines-combined-December-2022.pdf

Eligible data breach: unauthorised access, disclosure or loss of personal information.

Explicit Supporter Permission: means consent given explicitly in writing or orally. This could include a handwritten signature, an oral statement, or voice signature to signify agreement.

Loss: accidental or inadvertent loss of personal information held by TAI in circumstances where it is likely to result in unauthorised access or disclosure, e.g. leaving a laptop or USB on the train

Notifiable Data Breaches Scheme – the scheme introduced under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)

Personal Information: is defined as any information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

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

Unauthorised access: when a person accesses personal information that they were not supposed to, e.g. an employee accessing financial records of another colleague due to personal curiosity, a phone volunteer looking at child partner data when it is not relevant

Unauthorised disclosure: when personal information is made accessible or visible to others outside TAI

Related Policies and Procedures

This Policy should be read in conjunction with the following: -

- Complaints Handling Policy
- Fraud Control Policy
- Child Safe Policy
- Notifiable Data Breaches Procedure
- Business Continuity Policy
- Crisis Management Plan
- Website Rules

External References

- Privacy Act 1988 (Cth)
- Australian Privacy Principles Guidelines
- The Australian Privacy Principles

Document Control Information

Privacy Policy	
Owner	Director Governance, Risk and Business Optimisation
Master Copy	Policy QA Coordinator
Date created	2011
Date last reviewed	15/5/2025
Approved by Director of Governance, Risk and Business Optimisation	
Approved by Executive/CEO	10/01/2018
Endorsed by FRC	31/01/2018
Approved by Board	25/05/2018
Date next Review	15/5/2028

Date	Version	Revision Description	Reviewed / Updated by
2011	1	Original version	Director of Business
01/04/2014	2	Update to reflect new Australian Privacy Principles	Privacy Committee/Director of Business
01/07/2016	3	Templated from BWAA version	Governance & Compliance Specialist
01/08/2016	4	Updated Disclosure Item (c) to accord with Fraud Control Policy	Governance & Compliance Specialist
07/09/2016	5	Updated 'How we collect and use personal information' to reflect current practice regarding how supporters can change what communication they receive	Policy QA Coordinator
15/12/2017	6	Updated to align with Australian Privacy Principles, include partner organisations and child partners more clearly Added Eligible Data Breaches Section	Governance and Compliance Specialist, Policy QA Coordinator & Privacy Committee
02/10/2018	7	Added new point c) under Disclosure section to capture overseas data storage.	Supporter Engagement Lead and Privacy Committee
15/5/2025	8	Updated to comply with Australian Privacy Principles	Risk & Governance Coordinator