Privacy Policy

Details

Policy & Procedure Owner	ERFA Board	
Approved by	ERFA Board of Directors	
Date Approved	**Date of Last Revision**	**Next Review**
August 2015	August 2022	August 2024

Abbreviations

ACFID	Australian Council for International Development
APPs	Australian Privacy Principles
ERFA	Edmund Rice Foundation Australia
PCI DSS	Payment Card Industry Data Security Standards

Definitions

Associates	Anyone in the community who interacts with ERFA Staff and Partners
ACFID Member	A not-for-profit organisation that has obtained accreditation with ACFID
Board Member	A volunteer director responsible for the strategic oversight of Edmund Rice Foundation
Cookie	A 'cookie' is a small amount of data generated by a website and saved to the web browser of a computer user when they visit that site. Cookies are used by web browsers to save a user's preferences for a particular website. Every time the user visits that website basic data such as their IP address, their web browser, the dates they visited the website and the pages they visited are sent from the web browser to the website.
Donors	Members of the public who contribute to ERFA in cash or in kind
Partner	Any organisation which has an MOU / contract with / or receives funding from ERFA
Program	Programs are overarching development approaches and initiatives that set priorities and guide project outcomes, results and activities. Programs can comprise ministries or entities
Projects	Projects are the development activities of a Program supported by ERFA
Project Beneficiaries	Children and adults who participate in and benefit from ERFA-funded programs
Staff	Employees, contractors, subcontractors, outworkers, apprentices and trainees, work experience students, volunteers, employers and any other person who performs work for ERFA or ERFK

Contact information

Chief Executive Officer	Bren Arkinstall - barkinstall@edmundrice.org
Privacy Officer and Programs Director	Emily Faller – ejfaller@edmundrice.org
ERFA Board Chair	Paul Gallagher – chair@erf.org.au
ERFA	www.erf.org.au or +61 7 3621 9649
ACFID	http://www.acfid.asn.au or +61 6 02 6285 1816

Contents Page

1.0 Introduction

Edmund Rice Foundation (Australia) (ERFA) is committed to protecting the privacy of all of its stakeholders, including Staff, Board members, Partners, Project Beneficiaries, Donors and any other Associates who otherwise interact with ERFA or its programs. We ensure that our methods of private information management are transparent at all stages of the information collection, usage and storage process. The information contained within this policy is in accordance with the Australian Privacy Act (1988) and the Australian Privacy Principles (APPs) enclosed within the Act. This policy indicates sections where conditions of one of the 13 APPs are satisfied.

2.0 Purpose

The purpose of this policy is to provide a framework for ERFA in dealing with privacy considerations. ERFA's Privacy Policy is based on the principles of free, prior and informed consent.

2.1 Free, prior and informed consent

ERFA's definition of consent:

- **Free:** the contributor experiences no coercion or manipulation in providing consent for the collection, storage and disclosure of their personal information. The most appropriate form of consent (i.e., written, vocal) commensurate to the context is solicited from the contributor. The contributor is in a position to comprehend the process and understand their rights in approving or refusing consent. If consent is being provided by a guardian on behalf of a contributor, the guardian can be reasonably deemed as having the contributor's safety and wellbeing at heart.
- **Prior:** consent is sought sufficiently in advance of authorisations or disclosures of personal information. Sufficient time is provided between a contributor providing their consent and the disclosure of their personal information to allow them to withdraw their consent.
- **Informed:** the contributor is provided with all information relevant to their disclosure. They are not deceived by the information collector either deliberately or by omitting pertinent information. The contributor is informed of their ability to remain anonymous if they prefer. The contributor is provided with a reasonable account of the purposes of disclosing their personal information. The contributor is provided with a reasonable account of the audience profile who may be privy to their personal information.

3.0 Scope

This policy makes a distinction between ERFA's stakeholder categories of: Staff, Board Members, Partners, Program Beneficiaries and Donors. The organisational relationship that ERFA maintains with its Staff, Board Members and Partners, including matters of information collection and privacy protection, is made explicit to them. The information collected from these stakeholders is critical to the functioning of a secure and honest workplace; as such, Staff, Board Members and Partners are unable to refuse the collection of certain personal information such as criminal record checks and employment history. Details of the organisation-employee relationship are further enclosed within ERFA's Human Resources Policy.

Project Beneficiaries represent ERFA's most vulnerable stakeholder category. Hence, extra precautions are taken to secure their personal information: they are entitled to refuse the collection of their personal information of any kind. The information collected from a select few of these stakeholders is typically of a statistical nature, used to provide insight into the impact of ERFA's programs, or of an anecdotal nature, used for marketing communications.

Compared to other stakeholders, Donors maintain a more customer-oriented relationship with ERFA; as such, donors might interact with ERFA without knowledge of our organisation's specific privacy policies.

4.0 Collection and usage of information

4.1 Soliciting of personal information

ERFA collects solicited personal information directly from our stakeholders when they make contact with us through various channels, including in-person, online, over the phone or in written form. As part of these channels stakeholders acknowledge that their information is being solicited, collected, used and stored in accordance with this Privacy Policy (APP 3).

ERFA takes reasonable steps to ensure that stakeholders are informed when their information is being collected (APP 5). In these instances stakeholders are provided with the following information from ERFA:

- ERFA's contact details;
- the nature of the information and the manner in which it was collected;
- whether ERFA's collection of information is authorised by law;
- the reasons ERFA collected personal information;
- the consequences for ERFA if personal information is not collected;
- ERFA's usual disclosure procedures of collected information;
- reference to ERFA's Privacy Policy; and
- whether ERFA is likely to disclose personal information to overseas recipients.

4.1.1 ERFA Clause for Collection of Personal Information (see page 18)

Such information is consolidated into a clause visible on the ERFA website by navigating through the pages: [About] – [Policies] – [Privacy Policies]. The clause is included below:

"Edmund Rice Foundation (Australia) is committed to the lawful collection of personal information under the Australian Privacy Act (1988). We collect personal information for marketing and communications purposes. Without such information we are unable to conduct stakeholder engagement and fundraising activities to the best of our ability. By visiting our website, making a donation, signing up to our newsletter, filling out a survey, applying for employment, or providing us with your information by any other means, you agree to the collection, usage, disclosure and storage of, and access to your personal information, as contained in our Privacy Policy. ERFA does not disclose personal information to any overseas recipients. For further enquiries regarding our privacy measures or to update your personal information please contact us at +61 7 3621 9649 or info@erf.org.au."

4.1.2 Shortened ERFA Clause for Collection of Personal Information

A shortened version of this clause, including a link to ERFA's full Privacy Policy, is included within all communications distributed to stakeholders where it is reasonable to do so, such as within online and written communications. The shortened clause is provided below:

"Edmund Rice Foundation (Australia) is committed to the lawful collection of personal information under the Australian Privacy Act (1988). For further enquiries regarding our privacy measures or to update your personal information please see our Privacy Policy or contact us at +61 7 3621 9649 or info@erf.org.au"

Stakeholders who contact an ERFA representative in-person or over the phone will be directed to ERFA's Privacy Policy webpage if they have enquiries relating to the collection of personal information.

4.2 Staff, Board Members and Partners

Personal information that ERFA may collect from Staff, Board Members and Partners includes:

- personal details such as name, signature, or date of birth;

- contact details; and
- employment history, educational qualifications, tax file numbers and volunteering history – with respect to prospective employees and volunteers.

Such information is reasonably necessary for ERFA to liaise with and to assess the employment credentials of its Staff, Board Members and Partners. ERFA does not collect sensitive information from any of its stakeholders, excepting Staff, Board Members and Partners who are subject to a criminal record check (APP 3). All Staff, Board Members and Partners are asked for their consent before conducting a criminal record check (APP 3). Parties that refuse to the collection of this information will not be permitted to work for or alongside ERFA. ERFA maintains separate policies that pertain to the collection and security of the personal information of our Staff, Board Members and Partners, as contained in our Human Resources Policy.

4.3 Project Beneficiaries

Personal information that ERFA may collect from Project Beneficiaries includes:

- personal details such as name;
- on a limited basis, contact details such as phone number or email address;
- the location and nature of the ERFA-affiliated project the beneficiary is engaged in;
- images and video footage of project beneficiaries;
- 'stories': personal accounts of a project beneficiary's experience with an ERFA-affiliated project; and
- sensitive information such as a Beneficiary's health status. ERFA ensures that the express consent of a Beneficiary is obtained when collecting such sensitive information (APP 3).

Such information is reasonably necessary for ERFA to conduct impact reporting and fundraising activities. Impact reports are necessary to monitor the success of ERFA projects. On occasion, surveys of Project Beneficiaries are necessary to gauge the reception of our projects and identify areas for improvement. Likewise, impact reports are critical to communicate our efforts to Donors and maintain transparency. In particular, anecdotal impact evaluations, the type we obtain by collecting images of and individual 'stories' from our Project Beneficiaries, are the most successful at spurring Donor engagement.

A child or their guardian must give their free, prior and informed consent for ERFA to collect and publish their personal information and identifying images for communications purposes. They can do this by either:

- signing a locally-translated copy of ERFA's Story & Image Use Consent Form (see page 16) which permits ERFA to use their personal information (unless consent is withdrawn) and without compensation.

When soliciting consent to use a Beneficiary's image, video or story, details should be provided as to how and where their image, video or story might be used, such as in social media posts, supporter newsletters, quarterly impact publications and annual impact publications. The Beneficiary must also be informed of their ability to decline consent without negative impacts and use a pseudonym when filling out surveys, providing a 'story' or otherwise engaging us in one-off correspondence.

4.4 Donors

Personal information that ERFA may collect from donors includes:

- personal details such as name, signature, or date of birth;
- contact details;
- payment details; and
- donation history.

Such information is reasonably necessary for ERFA to process donations and to send relevant

information to donors such as tax-deductible receipts and remittance advices. ERFA has limited access to donors' payment details, restricted to information necessary for identification purposes, such as the last 4 digits of a donor's payment card; the remainder of a donor's payment details are encrypted. ERFA maintains a register of the personal, contact and payment details of its historical donors. Donors have the option to deal with ERFA on an anonymous basis or to use a pseudonym when making a donation or otherwise engaging us in one-off correspondence (APP 2). Donors are entitled to decline the collection of their personal information by contacting ERFA directly. ERFA's contact details are clearly displayed in the ERFA Clause for Collection of Personal Information (see section 4.1.1). However, donors that wish to initiate an ongoing relationship with ERFA, or to receive payment information such as tax-deductible receipts may have to provide us with their personal details. ERFA does not collect sensitive information from any of its donors (APP 3).

4.4.1 Direct marketing:

Such information is also reasonably necessary for ERFA to perform fundraising and direct marketing activities (APP 3). ERFA uses donor's personal information to conduct direct marketing (APP 7). Direct marketing may include contacting our stakeholders via email, postage or phone call. For example, ERFA may wish to send newsletters, publications and event communications to donors. Donors are able to opt out of receiving direct marketing communications at any time by contacting ERFA on +61 7 3621 9649 or info@erf.org.au (APP 7).

4.5 Website visitors

Personal information that ERFA may collect from website visitors includes:

- Personal details such as name, signature, or date of birth
- Contact details
- Statistical data such as IP address, web browser, or website pages visited

ERFA tracks the traffic patterns of all website visitors through the URL registered to us. By navigating our website, website visitors' basic data can be tracked through the use of Cookies. Cookies sent to the ERFA website do not enable us to view a visitor's personal information. Rather, cookies provide useful aggregate diagnostics such as total website visitors and the most visited pages. Such information is reasonably necessary for ERFA to perform marketing and communications operations effectively and to continue to optimise our site for the benefit of our stakeholders. We may provide such information to third parties, but are not permitted to disclose visitors' personal information without first obtaining their consent (see section 2.1). Visitors are able to disable their web browser from accepting cookies, however certain functions of the ERFA website might become unavailable as a result.

4.6 Immersion participants

Personal information that ERFA may collect from its immersion participants includes:

- personal details such as name, signature, or date of birth;
- contact details; and
- sensitive information such as passport details. ERFA ensures that the express consent of immersion participants is obtained when collecting such sensitive information (APP 3).

ERFA occasionally conducts immersions to our overseas programs. To handle the booking details of and ensure the security of immersion participants, ERFA will collect and disclose their passport details to the Australian Government's SmartTraveller website and to our registered insurance company.

4.7 Collection of unsolicited information

In the event that an ERFA representative receives personal information that was not solicited by the entity that it concerns, and that information could not otherwise have been collected in a solicited manner in accordance with ERFA's Privacy Policy, the representative will either lawfully destroy of said information or de-identify it as soon as is reasonably possible (APP 4).

5.0 Disclosure of information

ERFA does not disclose personal information about its stakeholders to any other entity except in the following circumstances (APP 6):

- to disclose a Staff or Board member's name, contact or employment details on official ERFA correspondence;
- to disclose a project beneficiary's name, image, or story to ERFA's network of donors for the purposes of marketing and communications material; and
- to disclose a donor's payment details to their bank or financial institution.

In each of these instances consent to disclose private information is either explicitly, or when reasonable to do so, implicitly obtained from the stakeholder in question.

ERFA may disclose personal information about its stakeholders, including sensitive information, in the following exceptional circumstances (APP 6):

- When it is permitted or required to do so by law such as to avoid an imminent threat to a person's life or to public safety.
- When ERFA reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

In these instances an ERFA representative must make a written note of the use or disclosure of personal information.

5.1 Disclosure of information to an overseas entity

ERFA will not send personal information about an individual to any location outside Australia without first obtaining the consent of the individual (APP 8).

5.2 Disclosure of government-related identifiers

ERFA will not use or adopt the government related identifiers of its stakeholders to refer to them. ERFA will not disclose the government related identifiers of its stakeholders, such as Medicare numbers, Australian Passport numbers or driver license numbers, to any entity (APP 9).

6.0 Access

6.1 Ensuring the quality of personal information

ERFA takes reasonable steps to ensure that the personal information it collects, uses and discloses is accurate, up-to-date, complete and relevant. Information quality verifications are made at the time information is first collected (APP 10, 13).

6.2 Allowing stakeholders to access their personal information

ERFA's maintains an Open Information Policy and will take all necessary steps to respond to stakeholder's requests for information. Stakeholders have a right to access the personal information that ERFA holds about them and to advise ERFA of any perceived inaccuracy. To gain access to their information a stakeholder must verify their identity to an ERFA stakeholder (exceptions where ERFA is entitled to refuse a stakeholder access to their personal information is outlined in APP 12 under section 12.34). When a stakeholder advises an ERFA representative of a perceived inaccuracy in their stored personal information, ERFA will correct its records as soon as is practically possible. A small fee may be charged to cover the cost of verifying applications and locating, retrieving, reviewing and copying material requested. Cases where ERFA is entitled to charge for the cost of information retrieval are outlined in APP 12 under section 12.78.

ERFA's Database Coordinator will be the first point of contact for inquiries about privacy issues for

individuals wishing to make an inquiry or complaint regarding privacy.

7.0 Storage and security of personal information

7.1 Storage of personal information

ERFA does not hold personal information longer than necessary: the point when ERFA no longer has reasonable cause to use or disclose that information. When this point is reached an ERFA representative will take steps to either lawfully destroy of said information or de-identify it as soon as is reasonably possible. ERFA destroys hard-copy information by shredding it. ERFA destroys electronic information by deleting it from its databases in a way that is irretrievable (APP 11).

7.2 Security of personal information

ERFA holds personal information securely through physical and electronic means and will take all reasonable steps to ensure that personal information is protected from misuse, interference and loss, and from unauthorised access, modification and disclosure. Physical means to secure personal information include locked storage of paper records. Electronic means to secure personal information include password access rights to electronic records. ERFA stores electronic data in its online database, which is a secure file sharing and transfer service for business. Staff members are granted permission by ERFA's administrator to access files according to their individual clearance levels. ERFA Staff are required to respect the confidentiality of personal information and the privacy of stakeholders. Such requirements are communicated to ERFA Staff in Staff training (APP 11).

7.3 Responding to data breaches

In accordance with the Privacy Act (1988), ERFA has various strategies in place to respond to a data breach of the personal information of its stakeholders. A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost. By maintaining compliance to all 13 of the APPs ERFA systematically reduces the risk of a data breach.

Complying with the Notifiable Data Breach (NDB) scheme as contained in Part IIIC of the Privacy Act (1988), ERFA will notify the individuals affected and the Commission in the event of certain instances of a data breach:

- There is unauthorised access to or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

In the event of uncertainty whether an eligible instance of data breach has occurred, ERFA will conduct an internal assessment to determine whether the steps of the NDB scheme need be followed.

8.0 Transparency

8.1 Disclosing information to the public

ERFA maintains a commitment to transparency in the information it discloses to the public. As a not-for-profit organisation that funds its projects through the benevolent donations of its donor network, and that carries out operations in diverse countries to assist vulnerable communities of beneficiaries, ERFA's stakeholders have a right to access information regarding ERFA's impact and operations. Information that ERFA publicly discloses to its stakeholders and the wider public include the following regular publications: the Annual Report, the Annual Financial Report, the Impact Report (annual) and a biannually printed newsletter. These (and historical publications) are accessible from the ERFA website.

ERFA also disseminates information pertaining to its operations in monthly email newsletters, press releases and through its website and social media channels. Within these publications and content updates ERFA makes regular use of the 'stories' provided to it by project beneficiaries (see section

5.3). Only when the stipulations set out in this Privacy Policy have been met is the personal information regarding one of ERFA's project beneficiaries used and disclosed (see sections 5.3).

8.2 Inviting feedback from the public

To aid in its commitment to transparency and an Open Information Policy ERFA actively seeks feedback from its stakeholders. ERFA recognises the value in all types of feedback from its stakeholders. All of ERFA's physical publications include organisational contact details for stakeholders to use if they wish to submit feedback. Depending on the nature of the feedback submitted and the organisational departments it relates to, an ERFA representative will strive to respond to the stakeholder as soon as is reasonably possible. For further details regarding ERFA's handling of complaints, see ERFA's Complaints Handling Policy.

9.0 Payment card security

ERFA is committed to the ongoing security of cardholder data. ERFA takes every step to be compliant with the Payment Card Industry Data Security Standards (PCI DSS). Contained below are some recommendations for maintaining PCI DSS compliance.

9.1 Develop program, policy and procedures

ERFA uses a payment gateway, *Payments2Us*, to process virtual credit card information. When a donor makes a contribution to ERFA their credit card information is transferred from the payment gateway to ERFA's designated bank, *Commonwealth Bank of Australia*. All of this data is encrypted and cannot be accessed by ERFA employees. The privacy policy of Payments2Us can be viewed from: https://www.payments2us.com/privacy/.

9.2 Assign ownership for coordinating security activities

ERFA's Database Coordinator is the sole person permitted to coordinate data security activities. The Database Coordinator's responsibilities include updating the personal information of donors and contacting donors in the event of a failed payment. Donors' personal information that the Database Coordinator has access to includes personal details such as name, signature and date of birth, contact details, payment details and donation history (See Section 4.4 Donors).

9.3 Detect and respond to control failures

In the event of an unsecure payment the Database Coordinator will receive an automated notification from Payments2Us via ERFA's designated CRM, *Salesforce*. To solve the issue the Database Coordinator will review the notification and notify the relevant parties, including the donor themselves and *Payments2Us*. To contact the donor directly the Database Coordinator Contact will access the donor's personal information, such as their contact information. The only payment details that the Database Coordinator has access to includes those necessary for identification purposes, such as the last 4 digits of a donor's payment card; the remainder are encrypted (See Section 2.4 Donors).

9.4 Evolve the compliance program to address changes

ERFA's Privacy Policy will be reviewed every two years. ERFA Board will manage the review and evaluate the relevance and quality of ERFA's data security measures. Changes to data security will be implemented where ERFA no longer complies with the PCI DSS.

10.0 Data Breach Response Plan

A data breach can take many forms and have many causes. Depending on the circumstances, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference. ERFA's notification obligations can also vary.

Refer to the Notifiable Data Breach Response Plan at Appendix 1 of this Policy to manage suspected or known data breaches.

11.0 Related Documents/Policies

11.1 Related policies

- Child Protection Policy
- Complaints Handling Policy
- Human Resources Policy

10.2 Related documents

- Notifiable Data Breach Response Plan
- Image & Story Use Consent Form
- Program Story Form
- Questionnaire Forms
- ERFA Clauses for Collection of Personal Information

Notifiable Data Breach Response Plan

A data breach can take many forms and have many causes. Depending on the circumstances, the extent of interference with personal information will vary, as will the harm suffered by the individuals affected by the interference. Our notification obligations can also vary.

Suspected or known data breach

A data breach occurs when personal information held by Edmund Rice Foundation Australia (ERFA) is misused, interfered with, lost or subject to unauthorised access, modification or disclosure.

1. Contain

The first step is to **contain** a suspected or known breach, where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

2. Assess

The Organisation needs to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If there are reasonable grounds to believe this is the case, then the Organisation must notify.

If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, the Organisation should consider whether **remedial action** is possible. The Organisation will conduct an assessment in three stages:

1. **Initiate:** plan the assessment and form a DBRT
2. **Investigate:** gather relevant information about the incident to determine what has occurred
3. **Evaluate:** make an evidence-based decision about whether serious harm is likely. This decision should be documented.

The Organisation must conduct this assessment within 30 days.

Take remedial action

Where possible, the Organisation should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised databases.

If remedial action is successful in making serious harm no longer likely, then notification is not required. Progress to Step 4: Review.

NO — **Is serious harm still likely?** — **YES**

3. Notify

Where **serious harm is likely**, the Organisation must prepare a statement for the OAIC to be submitted as soon as practicable that contains:

- the Organisation's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

The Organisation must also notify affected individuals and inform them of the contents of this statement.

The Organisation has three options for notifying:

1. Notify all individuals
2. Notify all individuals at risk of serious harm.

OR if 1 or 2 aren't practicable:

3. Publish the statement on the Organisation's public website and publicise it.

The Organisation may provide further information in its notification, such as an apology and an explanation of what they are doing about the breach.

4. Review

Review the incident and take action to prevent future breaches. This may include:

- fully investigating the cause of the breach
- developing a prevention plan
- conducting audits to ensure the plan is implemented
- updating security/response plans
- considering changes to EREA policies and procedures
- revising staff training practices
- consider a report to the EREA Board on outcomes and recommendations following the review

The Organisation should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC
- professional bodies
- other entity/ies that may be involved in the breach