



Privacy Policy

Policy & Procedure Owner	ERFA Board	
Approved by	ERFA Board of Directors	
Date Approved	Date of Last Revision	Next Review
	August 2015	November 2016

The Edmund Rice Foundation (ERFA) is committed to both protecting and securing the privacy and confidentiality of the personal information of donors.

This policy provides the information that the Privacy Act requires us to communicate to all of our Donors.

Collection of information

Personal information held by ERFA may include:

- donors name
- contact details (address, phone, fax, email)
- bank account or credit card details if provided
- donation history.

If a donor chooses not to provide ERFA with their contact details when they donate to ERFA, ERFA is unable to send an official tax-deductible receipt and letter of thanks.

ERFA collects personal information directly from donors, when they provide it over the phone, the website or on a donation form when making a donation to ERFA.

Use of information

ERFA does not make any use of the personal information it receives from donors except to:

- process any donations; and
- send to donors information about ERFA for example, newsletters

Arrangements have been made for donors to easily advise ERFA if they no longer wish to receive information.



Disclosure of information

ERFA does not disclose information about its donors to any other organisation except:

- in the case of a donor's bank or financial institution in the case of direct debit or a credit card transaction;
- where permitted or required by law; in a case to avoid an imminent threat to a person's life or to public safety.

ERFA holds personal information securely through physical and electronic means. We will take all reasonable steps to ensure that your personal information is not misused, lost or subject to unauthorised access or use.

Access

Under new privacy requirements, donors have a right to access the personal information that ERFA holds about them.

ERFA will correct its records containing personal information as soon as practically possible, at the request of the individual concerned in accordance with the Privacy Act.

A small fee may need to be charged for searching for and providing you with access to your personal information.

ERFA's Donor Relations Manager will be the first point of contact for inquiries about privacy issues for individuals wishing to make an inquiry or complaint regarding privacy.

Privacy complaints will be managed in accordance with Foundation's Complaint Handling Policy.

Website

ERFA will allow its customers to transact with it anonymously wherever that is reasonable and practicable.

ERFA will not make it mandatory for visitors to its web sites to provide Personal Information unless such personal information is required to answer an inquiry or enable them to make a donation to ERFA.

ERFA may however request visitors to provide personal information voluntarily to Foundation (for example, as part of a competition or questionnaire).

Disclosure of personal information

ERFA may disclose personal information, including sensitive information, held about an individual to:

- government departments;
- medical practitioners in life threatening situations;
- anyone appropriately authorised
- bodies with legal entitlements to the information.



When relevant, the individual's consent will be obtained prior to the disclosure of personal information.

Sending information overseas

ERFA will not send personal information about an individual outside Australia without obtaining the consent of the individual (in some cases consent will be implied) or otherwise complying with the National Privacy Principles.

Management and security of personal information

ERFA staff are required to respect the confidentiality of personal information and the privacy of individuals. ERFA has in place steps to protect the personal information ERFA holds from misuse, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and passworded access rights to computerised records.

Updating personal information

ERFA endeavours to ensure that personal information it holds is accurate, complete and up-to-date. Individuals may seek to update their personal information by contacting the Donor Relations Manager in writing at any time.

The National Privacy Principles require ERFA not to store personal information longer than necessary.

The right to check what personal information is held by ERFA

Individuals have the right to obtain access to any personal information that ERFA holds about them and to advise ERFA of any perceived inaccuracy with some limited exceptions. Requests to access any information the Foundation holds should be directed to the Province Leader in writing.

ERFA may verify an applicant's identity and specify what information it will provide. A fee may be charged to cover the cost of verifying applications and locating, retrieving, reviewing and copying material requested. If the information sought is extensive, ERFA will advise the likely cost in advance.

Appendix A Privacy Act 1988 Schedule 3—National Privacy Principles

1 Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of the organisation and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected; and
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
 - (e) any law that requires the particular information to be collected; and
 - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.
- 1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:
 - (a) both of the following apply:
 - i. the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
 - ii. the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
 - (b) the individual has consented to the use or disclosure; or
 - (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - i. it is impracticable for the organisation to seek the individual's consent before that particular use; and
 - ii. the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - iii. the individual has not made a request to the organisation not to receive



EdmundRice
FOUNDATION
AUSTRALIA

- direct marketing communications; and
- iv. in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
 - v. each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
- i. it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - ii. the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - iii. in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
- i. a serious and imminent threat to an individual's life, health or safety; or
 - ii. a serious threat to public health or public safety; or
- (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (g) the use or disclosure is required or authorised by or under law; or
- i. the organisation reasonably believes that the use or disclosure is reasonably necessary for
 - ii. the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - iii. the enforcement of laws relating to the confiscation of the proceeds of crime;
 - iv. the protection of the public revenue;
 - v. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - vi. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.



Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.
- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
- (a) the individual:
 - i. is physically or legally incapable of giving consent to the disclosure; or
 - ii. physically cannot communicate consent to the disclosure; and
 - (b) a natural person (the carer) providing the health service for the organisation is satisfied that either:
 - i. the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - ii. the disclosure is made for compassionate reasons; and
 - (c) the disclosure is not contrary to any wish:
 - i. expressed by the individual before the individual became unable to give or communicate consent; and
 - ii. of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
 - (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).
- 2.5 For the purposes of subclause 2.4, a person is **responsible** for an individual if the person is:
- (a) a parent of the individual; or
 - (b) a child or sibling of the individual and at least 18 years old; or (c) a spouse or de facto spouse of the individual; or
 - (c) a relative of the individual, at least 18 years old and a member of the individual's household; or
 - (d) a guardian of the individual; or
 - (e) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
 - (f) a person who has an intimate personal relationship with the individual; or
 - (g) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

- (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
- (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
- (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
- (d) the request for access is frivolous or vexatious; or
- (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or



EdmundRice
FOUNDATION
AUSTRALIA

- (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- (g) providing access would be unlawful; or
- (h) denying access is required or authorised by or under law; or
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - i. the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - ii. the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - iii. the protection of the public revenue; or
 - iv. the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 - vi. by or on behalf of an enforcement body; or
- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and

6.6 If the individual and the organisation disagree about whether the information is



EdmundRice
FOUNDATION
AUSTRALIA

accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency; or
- (b) an agent of an agency acting in its capacity as agent; or
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

- 7.2 However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

- 7.3 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
- (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
- (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

- 7.4 In this clause: **identifier** includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an **identifier**.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to



EdmundRice
FOUNDATION
AUSTRALIA

- the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
- (f) the transfer is for the benefit of the individual;
- (g) it is impracticable to obtain the consent of the individual to that transfer;
- (h) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (i) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required by law; or
- (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - i. is physically or legally incapable of giving consent to the collection; or
 - ii. physically cannot communicate consent to the collection; or
- (d) if the information is collected in the course of the activities of a non-profit organisation— the following conditions are satisfied:
 - i. the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - ii. at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
- (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

- (a) the information is necessary to provide a health service to the individual; and
- (b) the information is collected:
 - i. as required by law (other than this Act); or
 - ii. in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an



individual if:

- (a) the collection is necessary for any of the following purposes:
 - i. research relevant to public health or public safety;
 - ii. the compilation or analysis of statistics relevant to public health or public safety;
 - iii. the management, funding or monitoring of a health service; and
- (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - i. as required by law (other than this Act); or
 - ii. in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - iii. in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause: **non-profit organisation** means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.