

INF Australia Privacy Policy v5

Version:	5	Developed:	December 2018
Owner:	Chief Executive Officer	Latest Revision:	June 2025
Users:	Staff, Board, Volunteers, Partners, Contractors, Ambassadors	Review date	June 2028

Policy complies with	Privacy Act 1998 Australian National Privacy Principles in Privacy Amendment (Private Sector) Act 2000 (Australian Privacy Principles) Australian Council for International Development (ACFID) Code of Conduct Payment Card Industry Data Security Standard Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 ¹
Related Policies	Artificial Intelligence Policy Code of Conduct Communications Policy Complaints Handling Policy Cyber Security Policy Fundraising Policy Risk Management Policy Transparency and Accountability Policy
Related Practice Documents	Incident Reporting Procedure

Table of Contents

1	Introduction	2
2	Purpose	2
3	Scope	2
4	Policy	3
5	Roles and Responsibilities	3

6	Process Guide.....	4
6.1	Collection	4
6.2	Collection of Information by Online Activity Cookies or Social Media	5
6.3	Use & Disclosure	6
6.4	Storage	8
6.5	Destruction & de-identification	8
6.6	Data Quality	8
6.7	Data Security and Retention	8
6.8	Eligible Data Breaches.....	8
6.9	Openness	10
6.10	Access and Correction.....	10
6.11	Identifiers	11
6.12	Anonymity.....	12
6.13	Making information available to other organisations.....	12
7	Relevant Legislation and Conventions	12
8	Policy Review.....	12
9	Contacting INFA.....	12

1 Introduction

Protection of privacy is important to International Nepal Fellowship Australia (INFA). It is committed to protecting the privacy and security of personal information which it collects, holds and administers. It is a requirement of the Australian Privacy Principles, established under the Privacy Amendment (Private Sector) Act 2000, that people about whom INFA holds information be informed about the information collected and held, and the use of this information. Personal information is information which directly or indirectly identifies a person.

2 Purpose

The purpose of this policy is to provide a framework for INFA to deal with privacy considerations.

3 Scope

This policy applies to:

- INFA personnel (being Board members or members of Board committees, employees, or volunteers or partners that INFA provides funding to); and
- Contractors engaged by INFA

INFA management will take steps to ensure that all INFA personnel and contractors are made aware of their obligations under this policy.

4 Policy

INFA collects and administers a range of personal information for fundraising and communications. It is committed to protecting the privacy of personal information it collects, holds and administers.

INFA recognises the essential right of individuals to have their information administered in ways which they would reasonably expect, both protected and made accessible to them. These privacy values are reflected in and supported by INFA's core values and philosophies, and also reflected in this policy, which is compliant with the Privacy Act 1988 (Cth) and National Privacy Principles.

INFA is bound by laws which impose specific obligations when it comes to handling information. It has adopted the following principles contained as minimum standards in relation to handling personal information.

INFA will

- Collect only information which it requires for its primary function;
- Ensure that stakeholders are informed as to why it collects the information and how it administers the information gathered;
- Use and disclose personal information only for the organisation's primary functions, a directly related purpose or for another purpose with the person's consent;
- Store personal information securely, protecting it from unauthorised access; and
- Provide stakeholders with access to their own information and the right to seek its correction.

5 Roles and Responsibilities

INFA's Board is responsible for developing, adopting and reviewing this policy.

INFA's Chief Executive Officer is responsible for:

- the implementation of this policy;
- monitoring changes in privacy legislation; and
- advising on the need to review or revise this policy, as required.

6 Process Guide

6.1 Collection

INFA will:

- Only collect information that is necessary for the performance and primary function of INFA.
- Collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- Notify stakeholders about why it collects the information and how it is administered.
- Notify stakeholders that this information is accessible to them.
- Collect personal information from the person themselves wherever possible.
- If collecting personal information from a third party, be able to advise the person whom the information concerns, from whom their personal information has been collected.
- Collect sensitive information only with the person's consent or if required by law. Sensitive information includes information about religious beliefs, race, gender and other characteristics.
- Also only collect sensitive information about an individual if such 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:
 - is physically or legally incapable of giving consent to the collection; or
 - physically cannot communicate consent to the collection; or
- Collect information during the course of its activities as a non-profit organisation, only if following conditions are satisfied:
 - the information relates solely to its members or to individuals who have regular contact with it in connection with its activities;
 - at or before the time of collecting the information, INFA informs the individual whom the information concerns that it will not disclose the information without the individual's consent; and
 - the collection must be necessary for the establishment, exercise or defence of a legal or equitable claim.
- Determine, where unsolicited information is received, whether the personal information could have been collected in the usual way. If it could have, it will be treated normally; if not, it will be destroyed and the person whose personal information was collected will be notified about the receipt and destruction of their personal information.

6.2 Collection of Information by Online Activity Cookies or Social Media

INFA uses online activity cookies and other analytics tools (such as internet tags, pixels, or web beacons) to collect information about how you interact with its website for a variety of reasons. In this policy, all these technologies are referred to as “cookies” or “analytics tools”

Cookies are small text files used to store information in web browsers or on your electronic device, which receive identifiers and other information related to your device. They can allow recall of data by a web server in the domain that place the cookie. Other analytics tools include pixels which operate in a similar way to cookies but allow INFA to send data related to multiple events and optimise its advertising performance.

Third party cookies may include:

- Social Media cookies designed to show you advertisements and content based on your social media profile and activities on INFA’s website;
- Analytics cookies to better understand how you and others use INFA’s website so that it can be made better, and so the third parties can improve their own products and services;
- Advertising cookies to show you INFA advertisements that are relevant to you; and
- Required cookies used to perform essential website functions. Where required, it obtains your consent prior to placing or using optional cookies that are not (i) strictly necessary to provide the website; or (ii) for the purpose of facilitating a communication.

INFA uses cookies or analytics tools to honour your preferences, provide interest-based advertising, improve the user web experience, provide it with web data analytics, improve its presentations and market these effectively. Its website may include web beacons, cookies, or similar technologies from third parties, such as Facebook acting on its behalf in advertising INFA’s activities.

When you visit INFA’s website, you can choose to reject analytics tools. If you do, only performance analytics will be conducted which do not collect personal information and also those tools which are required to make the website operate.

You can also take control over your personal information using one of the following options:

- Turning off or opting out of cookies, analytics, personalised ads
- You may be able to adjust your browser to turn off use of “cookies” or for it to notify you when cookies are being used. The <http://www.aboutads.info/choices> web pages provide useful information on your advertisement choices and how you can limit advertisement tracking.

However, if you disable cookies, you may not be able to access certain areas or take advantage of certain features on INFA’s website. Pixels can be managed directly with external parties (Facebook and Google) or by rejecting marketing cookies.

You can also adjust your advertisement options directly with the third-party platform.

- Facebook: via Ad Settings or Ad Preferences menu.
- Instagram: via Settings > Accounts Centre > Ads > Ad Preferences > Ad Settings.
- Google Analytics: <https://tools.google.com/dlpage/gaoptout/>.
- Linked-In: via Settings
- YouTube: via Settings

When you visit and interact with a third-party website, INFA recommends that you read that third party's privacy policy as any of the personal information provided and your interactions with that page are outside our control. You may also find information on how you can control targeted marketing or turn off some of these features.

6.3 Use & Disclosure

INFA will:

- Only use or disclose information for the primary purpose for which it was collected or for a directly related secondary purpose.
- For other uses, obtain consent from the affected person.
- In relation to a secondary purpose, only use or disclose the personal information where:
 - a secondary purpose is related to the primary purpose and the individual would reasonably have expected INFA to use it; or
 - the person has consented; or
 - certain other legal reasons exist, or disclosure is required to prevent serious and imminent threat to life, health or safety.
- In relation to personal information collected from a person, use the personal information for direct marketing, where that person would reasonably expect it to be used for this purpose, and INFA has provided an optout and the optout has not been taken up.
- In relation to personal information which has been collected other than from the person themselves, only use the personal information for direct marketing if the person whose personal information has been collected has consented (and they have not taken up the optout).
- In each direct marketing communication with the individual, INFA draws to the individual's attention, or prominently displays a notice, that they may express a wish not to receive any further direct marketing communications.
- State whether the information is to be sent overseas and further will ensure that any overseas providers of services are as compliant with privacy as INFA is required to be. Such disclosures will only be made if:
 - the overseas 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 the National Privacy Principles; or

- the individual consents to the transfer; or
 - the transfer is necessary for the performance of a contract between the individual and INFA, or for the implementation of pre-contractual measures taken in response to the individual's request; or
 - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between INFA and a third party; or
 - INFA 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.
- In relation to the overseas transfer of personal information, if it is impractical for INFA to receive the person's consent to that transfer, have sufficient reasons to believe that the person would likely give consent if they could have been contacted.
 - Provide all individuals access to their personal information, except where it is a threat to life or health, or it is authorised by law to refuse. If a person is able to establish that the personal information is not accurate, then INFA must take steps to correct it. INFA may allow a person to attach a statement to their information if it disagrees it is inaccurate.
 - Where for a legal or other reason, INFA is not required to provide a person with access to the information, consider whether a mutually agreed intermediary would allow sufficient access to meet the needs of both parties.
 - Make no charge for making a request for personal information, correcting the information or associating a statement regarding accuracy with the personal information.
 - For each written direct marketing communication with the individual set out INFA's business address and telephone number and, if the communication with the individual is made by email or other electronic means (including fax), a number or address at which INFA can be directly contacted electronically.
 - If the disclosure of sensitive information is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety and it is impracticable for INFA to seek the individual's consent before the use or disclosure and the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A of the Privacy Act, INFA may make such a disclosure.
 - If it has sufficient reason to believe that an unlawful activity has been, is being or may be engaged in, and the disclosure of personal information becomes a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, then it may make such disclosures.

- Possibly disclose personal information if its disclosure is mandated by an enforcement body or is required for the following:
 - 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;
 - the enforcement of laws relating to the confiscation of the proceeds of crime;
 - the protection of the public revenue;
 - the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

For the purpose of this clause, INFA must make a written note of any such use or disclosure.

6.4 Storage

INFA will:

- Implement and maintain steps to ensure that any personal information is protected from misuse and loss, unauthorised access, interference, unauthorised modification or disclosure.
- Before INFA discloses any personal information to an overseas recipient, including a provider of IT services such as servers or cloud services; establish that they are privacy compliant. INFA will have systems which provide sufficient security.
- Ensure that INFA's data is up-to-date, accurate and complete.

6.5 Destruction & de-identification

INFA will:

- Destroy personal information once it is not required to be kept for the purpose for which it was collected, including from decommissioned laptops and mobile phones.
- Change information to a pseudonym or treat it anonymously if required by the person whose information INFA holds. INFA will not use any government-related identifiers unless they are reasonably necessary for its functions.

6.6 Data Quality

INFA will take reasonable steps to ensure the information that it collects is accurate, complete, up-to-date and relevant to the functions it performs.

6.7 Data Security and Retention

INFA will only destroy records in accordance with this policy.

6.8 Eligible Data Breaches

An 'eligible data breach' arises when the following three criteria occur:

- unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information;
- any of the above activities is likely to result in serious harm to one or more individuals; and
- INFA has not been able to prevent the likely risk of serious harm with remedial action.

Examples of a data breach include when:

- a device containing donors' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person
- An 'eligible data breach' that triggers notification obligations, is a data breach that is likely to result in 'serious harm' to any of the individuals to whom the information relates. Serious harm may include serious physical, psychological, emotional, financial, or reputational harm.

Relevant matters to assist the assessment of serious harm include:

- the kind of information
- sensitivity of the information
- if the information is protected by one or more security measures
- the kind/s of person/s who have obtained, or who could obtain the information
- if a security technology or methodology was used in relation to the information and was designed to make the information unintelligible or meaningless to persons not authorised to obtain the information
- the kind/s of person/s who have obtained or who could obtain the information, who may have intentions of causing harm and to circumvent the security technology or
- the methodology; or
- the nature of the harm

Some kinds of personal information may be more likely to cause an individual serious harm if compromised, including:

- documents commonly used for identity fraud (Medicare card, driver licence, passport)
- financial information
- combination of types of personal information allowing more to be known about individuals

The specific circumstances of the data breach are relevant when assessing whether there is a risk of serious harm to an individual including:

- Whose personal information was involved in the breach? Some individuals are more vulnerable, increasing the risk of serious harm
- How many individuals were involved? The scale of the breach affects the likelihood of risks
- Do the circumstances of the data breach affect the sensitivity of the personal information?
- How long has the information been accessible?
- Is the personal information adequately encrypted, anonymised, or not easily accessible?
- What parties may/ have gained unauthorised access to the personal information intended for malicious purposes?

When INFA becomes aware that an eligible data breach has occurred the *Privacy Officer* will promptly organise the notification to individuals at likely risk of serious harm, where serious harm cannot be mitigated through remedial action.

The *Privacy Officer* will also notify the Office of the Australian Information Commissioner as soon as practical through a statement about the eligible data breach.

6.9 Openness

INFA will:

- Ensure stakeholders are aware of this policy and its purposes.
- Make this information freely available in relevant publications and on its website.
- On request by a person, 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.

6.10 Access and Correction

INFA will:

- Ensure individuals have a right to seek access to information held about them and to correct it if it is inaccurate, incomplete, misleading or not up to date.
- If the individual and INFA disagree about whether the information is accurate, complete and up-to-date, and the individual asks it to associate with the information a statement claiming that the information is not accurate, complete or up to date, then INFA will take reasonable steps to do so.
- Provide to the individual its reasons for denial of access or a refusal to correct personal information.

INFA can withhold the access of an individual to his/ her information if:

- providing access would pose a serious and imminent threat to the life or health of any individual; or
- providing access would have an unreasonable impact upon the privacy of other individuals; or
- the request for access is frivolous or vexatious; or
- the information relates to existing or anticipated legal proceedings between INFA and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- providing access would reveal the intentions of INFA in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- providing access would be unlawful; or
- providing access would be likely to prejudice an investigation of possible unlawful activity; or
- an enforcement body performing a lawful security function asks INFA not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

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

If INFA decides not to provide the individual with access to the information on the basis of any of the above-mentioned reasons, it will consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

INFA may charge for providing access to personal information. However, the charges will be nominal and will not apply to lodging a request for access.

6.11 Identifiers

INFA will not:

- adopt as its own identifier of an individual an identifier that has been assigned by any third party. It may, however, adopt a prescribed identifier by a prescribed organisation in prescribed circumstances.
- use or disclose the identifier assigned to an individual by a third party unless:
 - the use or disclosure is necessary for INFA to fulfil its obligations to the agency; or
 - the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

6.12 Anonymity

INFA will allow people from whom the personal information is being collected to not identify themselves or use a pseudonym unless it is impracticable to deal with them on this basis.

6.13 Making information available to other organisations

INFA can release information to third parties where it is requested by the person concerned.

7 Relevant Legislation and Conventions

INFA personnel and contractors must adhere to privacy legislation which includes the *Privacy Act 1988* and any privacy legislation applicable in Nepal.

8 Policy Review

This policy will be reviewed at least every three years, or as required, incorporating lessons learned.

9 Contacting INFA

Queries regarding INFA's privacy policy, or about personal information held, to its Privacy Officer may be made by email, phone, mail or in person:

Email: ausoffice@inf.org.au

Phone: 02 9411 1195

Mail: PO Box 5400

West Chatswood Nest NSW 1515

Office: 1 -5 View Street

Chatswood NSW 2067

Revision History

Date	No.	Summary of Changes	Sections changed	Authorised by:
December 2018	3	General review and revision		INFA Board
August 2023	4	General review and revision. Added section 2.9	2.2, 2.5, 2.9	INFA Board
June 2025	5	Major rewrite of most sections.	Most	INFA Board