Australian Government

NAIF
Northern Australia Infrastructure Facility

Privacy Policy

JULY 2024

Investing for impact in northern Australia

Find out more at
naif.gov.au

Contents

Document Purpose

The Privacy Policy outlines Northern Australia Infrastructure Facility's (NAIF) approach to collecting, using, and disclosing personal information. In managing privacy, NAIF implements the requirements of the *Privacy Act 1988 (Cth)*.

1. Scope of this Policy

This Policy applies to NAIF Board Members, employees, and contractors. For the purpose of this policy 'employees' includes each of these categories.

2. Policy Statement

NAIF collects personal information while undertaking its functions under the NAIF Act and Investment Mandate. NAIF may also collect personal information for secondary purposes such as developing, establishing, and administering business with other organisations in relation to the promotion and administration of functions under the NAIF Act and Investment Mandate.

NAIF is committed to protecting the personal information it holds and complying with the requirements of the Privacy Act and is subject to the Australian Privacy Principles (APPs). The APPs set out the standards, rights, and obligations in relation to handling, holding, accessing, and correcting personal information.

3. Private Information

3.1. Definitions of personal and sensitive information

The Privacy Act defines personal information as:

"Information or an opinion, whether true or not, and whether recorded in a material form of not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion"

Examples of personal information may include:

- Names and addresses;
- Banking details;
- Photographs (where identity can be reasonably ascertained); or
- Details that when put together can reasonably identify the individual.

Sensitive information as defined by the Privacy Act can include information regarding an individual's:

- Racial or ethnic origin;
- Political opinion / membership of a political association;
- Religious belief;
- Membership in a professional or trade association / union;
- Sexual preferences;
- Criminal record; and
- Health record.

3.2. Types of personal and sensitive information collected

In the ordinary course of business, NAIF collects:

- Information about users of NAIF's website, including the user's server address;
- Identification information about individuals including their name, mailing address, telephone, and email addresses';
- Financial and other personal information about individuals associated with project proponents; and
- In certain circumstances, sensitive information about individuals as required by other legislation such as employment (e.g., memberships, identification documentation, etc.).

When NAIF considers an investment proposal, NAIF will collect and store personal information.

Personal or sensitive information is collected by NAIF to comply with legislation such as, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and the *Archives Act 1983* (Cth).

NAIF recommends that individuals do not provide sensitive information to NAIF unless specifically requested by NAIF.

4. Information Collection

Personal information may be collected:

- Directly from the individual to whom the information relates, including by telephone and through paper and electronic documents completed by individuals authorised to provide the information to NAIF;
- From NAIF's representatives, advisers and third parties;
- From financiers and representatives of proponents to whom the information relates;
- From NAIF's records of contacts who have contacted NAIF, attended NAIF events, or subscribed to information published by NAIF;
- From publicly available sources; and
- From NAIF's website.

Privacy Collection Notices are provided when information is requested from individuals which details the specific use and disclosure of the information.

5. Information Disclosure

NAIF uses and discloses personal and sensitive information to carry out and fulfil its functions under the NAIF Act and Investment Mandate. This can include the following purposes:

- Assessing the suitability of an application for a financial product or service;
- Ongoing management of financial products and services;
- Management of supplier and stakeholder relationships, including requests for feedback;
- Assessing an individual's employment application and ongoing employment relationship;
- Provide updates on NAIF's services and activities;
- Conduct direct marketing, market research campaigns or stakeholder satisfaction research;
- Processing and responding to requests for information and complaints; and
- Taking any action, NAIF is required or authorised to by law.

Privacy Collection Notices are provided when information is requested from individuals which details the specific use and disclosure of the information.

NAIF also uses and discloses personal information for secondary purposes (e.g., for promotional opportunities and administration of its functions) that are otherwise permitted under the Australian Privacy Principles, including where:

- The individual consents;
- The individual would reasonably expect the use or disclosure and the secondary purpose is related to the primary purpose;
- The use or disclosure is required or authorised by law or court order; or
- The use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

NAIF discloses personal information to third parties located in Australia or overseas where it believes such disclosure is necessary to assist NAIF to fulfil its functions. For example, NAIF may disclose personal information to:

- Employees to fulfil their duties;
- Commonwealth, State or Territory government agencies and departments in accordance with the NAIF Act and any regulations or legislative instruments made under it;
- Comply with our obligations under law including the *Anti-money Laundering and Counter Terrorism-Financing Act 2006* and the *Freedom of Information Act 1982*;
- External advisers (for example, lawyers, accountants and auditors);
- Insurers and financiers (where required);
- External service providers engaged by NAIF to assist in performing its functions and duties;
- Comply with required laws, regulations or codes; and
- Comply with any other purpose as outlined to the consenting individual.

NAIF may disclose personal information to third parties by electronic means, including via the internet.

6. Information Storage and Retention

NAIF endeavours to protect personal information it holds from misuse, interference and loss and to protect it from unauthorised access, modification and disclosure.

Personal information obtained by NAIF is held on NAIF's cloud storage, and in instances where information is disclosed to third parties, on their cloud storage. NAIF has also implemented the following measures to protect personal information held by it:

- identity and access management systems;
- security obligations imposed on Board members, employees, contractors and consultants; and
- Privacy Policy training for all employees.

Where NAIF discloses personal information to third parties located in Australia or overseas, NAIF will take reasonable steps to ensure that those third parties treat the information in accordance with the Privacy Act and subject to NAIF's confidentiality requirements.

If NAIF becomes aware of a data breach or possible data breach, NAIF will act in accordance with the data breach response plan. NAIF will notify the Office of the Australian Information Commissioner and affected individuals of any data breaches which meet the criteria for an 'eligible data breach' as required by the Notifiable Data Breaches scheme (established under Part IIIC of the Privacy Act).

6.1. Contact and opting out

If you or a client of NAIF wishes to:

- obtain access to or seek correction of your personal information;
- opt out of receiving information;
- lodge a complaint about a breach of privacy;
- query how personal or sensitive information is collected or used; or
- ask questions about NAIF's Privacy Policy.

You may contact NAIF via the post or email. NAIF will assess that request and provide a response back to the requestor in a timely manner.

Post	Email
NAIF Privacy Officer **PO Box 4896** **Cairns, QLD 4870**	Privacy@naif.gov.au

7. Complaints

Any complaints relating to Privacy will be addressed through the NAIF External Compliant Handling Policy.

8. Reporting

All employees are required to use the Risk and Compliance system to report any incidents or near misses related to privacy or data breach matters. This includes but is not limited to situations where unauthorised access to personal data occurs, consent is not collected where required, or instances of non-compliance with the policy. Employees are encouraged to refer to the incident guideline on NAIF Connect or contact the Risk and Compliance team for any queries or concerns related to reporting procedures.

All situations that require immediate attention in the event of data breaches or disclosure of information, promptly escalate to the Privacy Officer and the IT Helpdesk. After escalation, ensure the incident is raised in the Risk and Compliance system.

9. Roles and Responsibilities

Role	Responsibility
NAIF Board	• Approving material policy changes after a review and recommendation by the Policy Sponsor. • Tasking management with policy implementation, exception reporting and for developing procedures to support the policy. • Complying with the requirements of this policy.
Chief Executive Officer	• Approving immaterial policy changes after a review and recommendation by the Policy Sponsor. • Complying with the requirements of this policy.
Chief Operating Officer	• Implementing this policy at NAIF. • Reviewing the Policy each calendar year. • Acting as the Privacy Champion.
Director, Risk and Compliance	• Providing training to employees on this policy. • Acting as the Privacy Officer.
Employees	• Complying with the requirements of this policy.

Where an employee fails to comply with the requirements set out in this policy, disciplinary action may be taken.

10. Review and Approval

The Chief Executive Officer approves the Policy every two years.

The Policy is reviewed annually (or more frequently if required) by the Policy Sponsor to ensure it remains aligned with legislation and good practice. If any material amendments occur to the Policy arising from the review cycle, it is provided to the NAIF Board for review and approval.

Document Review and Approval

Policy Sponsor	Policy Approver	Approval Date	Next Board Review
Chief Operating Officer	NAIF Board/CEO	July 2024	March 2026

Related Documentation

Privacy Act 1988 (Cth)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Archives Act 1983 (Cth)

External Complaint Handling Policy

Data Breach Response Plan

Privacy Collection Notices