|  |  |
| --- | --- |
|  |  |



Contents

[About this guide 3](#_Toc170142395)

[Part 1 – Privacy in Fundraising 1](#_Toc170142396)

[What does “privacy of personal information” mean in Australia? 1](#_Toc170142397)

[What is ‘personal information’? 2](#_Toc170142398)

[Are NFPs required to comply with the Privacy Act? 3](#_Toc170142399)

[What are the key obligations under the Privacy Act for NFPs? 4](#_Toc170142400)

[A to Z of key concepts under the APPs 8](#_Toc170142401)

[Privacy Law Reform in 2024 12](#_Toc170142402)

[Part 2 – Privacy in Practice 13](#_Toc170142403)

[Privacy program management 13](#_Toc170142404)

[Privacy policy and collection notices 14](#_Toc170142405)

[Assessing and managing privacy risks 16](#_Toc170142406)

[Direct marketing 18](#_Toc170142407)

[Managing personal information of beneficiaries 18](#_Toc170142408)

[Engaging third party service providers 19](#_Toc170142409)

[Overseas transfers 20](#_Toc170142410)

[Dealing with privacy complaints 21](#_Toc170142411)

[Data retention 22](#_Toc170142412)

[Data breaches 23](#_Toc170142413)

[Recommended privacy documentation 24](#_Toc170142414)

[Part 3 – Resources 25](#_Toc170142415)

[Glossary 25](#_Toc170142416)

[Resources and links 27](#_Toc170142417)

[Contact details 28](#_Toc170142418)

# 

## About this guide

This guide has been prepared to provide general guidance to organisational members of the Fundraising Institute of Australia (**FIA**) in the not-for-profit (**NFP**) sector who are undertaking fundraising activities.

The purpose of this guide is to provide:

* an overview of general legal requirements under the Privacy Act for handling of personal information, including obtaining consent, direct marketing activities, data retention and data breaches;
* best practice for NFPs to manage compliance with the Privacy Act, including identifying and managing risk; and
* recommended privacy-related documentation.

How to use this guide

This guide is divided into the following sections:

|  |  |  |
| --- | --- | --- |
| **No.** | **Title** | **What does this Part contain?** |
| **1** | **Privacy in Fundraising** | Introduction to the Privacy Act, including the Australian Privacy Principles.  Overview of key privacy concepts and legal requirements for NFPs under the Privacy Act.  Understanding obligations under the Privacy Act. |
| **2** | **Privacy in Practice** | Practical tips and best practice to assist NFPs to meet their obligations under the Privacy Act, using practical examples and case studies. |
| **3** | **Resources** | Additional resources, including a glossary and links to freely available resources and guidance on privacy law in Australia. |

Navigate using call-out boxes for:

**Snapshots** – high level summary of the key points in the section

**👍 Best practice tips** – practical application of the Privacy Act for FIA members

**Further information?** – additional resources or information for FIA members

Information in this guide can also be found using the table of contents and cross-references to commentary. Terms in blue text are defined in the Glossary in Part 3.

Scope and disclaimer

This guide focuses on privacy obligations set out in the *Privacy Act 1988* (Cth) (**Privacy Act**). NFPs may also have obligations under other laws, at both the state and territory level, and federal level (See Snapshot: Privacy Laws in Australia). While this guide makes references to the application of other laws, it does not provide guidance in relation to such other laws and is not intended to be a comprehensive guide for NFPs for all legal compliance matters.

This guide is intended to provide general guidance only and is not tailored to any specific FIA member. It does not deal with any sensitive information, such as health information, or other information collected in the member’s ordinary course of business, such as tax information or PI of volunteers, employees and suppliers.

Currency of this guide

This guide is current as at 30 June 2024. The Privacy Act is very likely to be reformed during 2024 and this guide will need to be read subject to those reforms.

## Privacy Law Reform in 2024

At the time of publication of this guide, it is anticipated there will be (potentially) significant reform to the Privacy Act in 2024, with the Commonwealth Attorney-General announcing a draft Bill is to be expected in August 2024.

It is unknown, at the time of publication, the precise nature or scope of the reforms to be addressed by the Bill.

However, the Bill is likely to reflect the proposed reforms agreed by the Government, and possibly also some of the reforms agreed-in-principle, in its response to the Attorney-General’s *Privacy Act Review Report 2022*. (The Government indicated that it is committed to introducing amending legislation in 2024 to address the 38 “agreed” proposals for law reform. However, while these proposals are “agreed”, the majority are either subject to further consultation or are to strengthen regulatory enforcement powers and other regulatory processes and guidance, rather than uplift protections or rights for individuals.)

The combination of the “agreed” and “agreed-in-principle” reforms, if implemented as proposed, would significantly impact information-handling practices of private and public sector entities (including NFPs).

In particular, the reforms propose an expanded definition of “personal information”, the introduction of a new overarching requirement that information handling practices be “fair and reasonable”, codification of a number of existing regulator positions with respect to consent, strengthening of children’s privacy, and changes to direct marketing practices.

NFPs will need to keep their privacy compliance program under review to meet any uplifted requirements implemented as part of these reforms. To prepare for the reforms, NFPs should consider:

* understanding what personal information it holds, where and how. This includes where personal information is held or otherwise handled by third party service providers.
* understanding current information handling practices and how it currently complies with its obligations under the Privacy Act. A privacy compliance audit or maturity assessment is a useful exercise to identify any gaps and other compliance and privacy risks.
* developing and implementing a roadmap to “up-lift” its existing privacy management framework. This includes updating practices, procedures and systems and conducting a privacy awareness program. The roadmap should include the “agreed” and the more-certain “agrees-in-principle” reforms that would impact the organisation, privacy awareness and training requirements, and projected future resourcing requirements.

# – Privacy in Fundraising

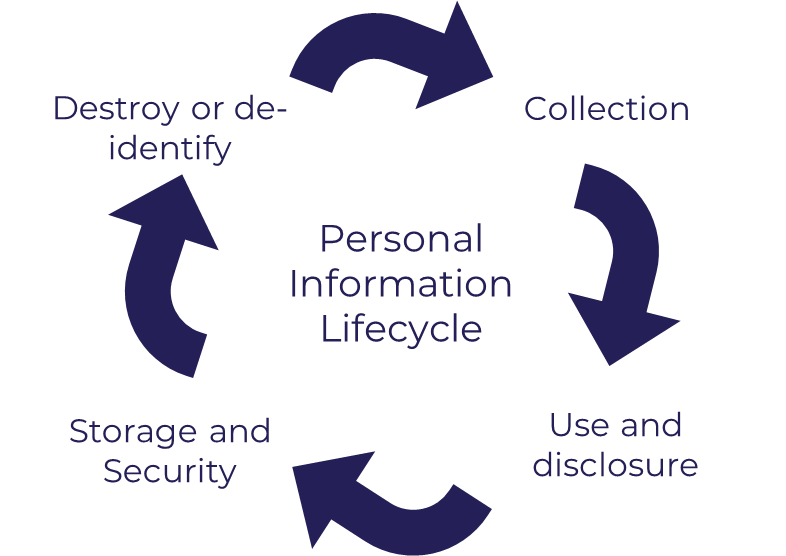
## What does “privacy of personal information” mean in Australia?

In this guide, ‘privacy’ refers to the obligations organisations and government agencies regulated by the Privacy Act have when handling personal information, and the rights individuals have under the Privacy Act.

|  |
| --- |
| **Snapshot: Privacy Laws in Australia**  The Privacy Act is the primary legislation in Australia that regulates the handling of personal information by the NFP sector. It is principles-based legislation, with the primary obligations contained in the 13 Australian Privacy Principles. It also contains mandatory data breach notification obligation for certain data breaches.  There are other privacy laws in Australia that may apply to an NFP, depending on the type of personal information or activity. For example, health information in New South Wales and Victoria is also subject to State-based privacy legislation. The handling of MyHealth Records is also subject to Commonwealth legislation. NFPs may also have contractual obligations to comply with other privacy laws, for example, under funding arrangements with government agencies.  There are also other laws in Australia that govern activities of NFPs that may involve handling personal information, such as surveillance and listening devices laws and regulations, workplace laws, consumer protection laws, human rights laws, and regulation of marketing activities, such as under the Spam Act, Do Not Call Register Act and the Corporations Act.  Currently, there is no broader general statutory “right to privacy” in Australia, although this is currently under review as part of the Privacy Act Reforms.  This guide only considers the Privacy Act. |

The Privacy Act primarily governs how personal information is handled through 13 Australian Privacy Principles (or **APPs**). The organisations and Commonwealth government agencies regulated by the Privacy Act are called “**APP entities**”.

The APPs govern how personal information is handled by APP entities across the information lifecycle.



Where an APP entity does not comply with the APPs, it will be an “interference with privacy” and there are potential penalties and other enforcement actions under the Privacy Act.

**Further information?** Refer to section Australian Privacy Principles [insert hyperlink].

## What is ‘personal information’?

|  |
| --- |
| **Snapshot:** Personal information is defined in the Privacy Act as information or opinion about an identified individual, or an individual who is reasonably identifiable. This includes whether or not the information or opinion is true, or recorded in material form or not. |

For NFPs, there may be a broad range of personal information that is collected and handled, such as information about donors, beneficiaries, volunteers and staff, as well as information that may be collected in the context of a fundraising campaign or charitable activity.

Information does not need to have a name attached to be “personal information”. It may include a person’s address, bank account details, photograph, information about an individual’s donations and bequests, their employer, or what the individual likes and their opinions.

Personal information does not include information about a company or a deceased person.

### ‘Reasonably identifiable’

Whether an individual can be identified or is ‘reasonably identifiable’ depends on the circumstances, including the nature and amount of information, who can access it, or whether information can be ‘linked’ to another piece of information, and the time and cost that would be involved in identifying them.

Some information may not be personal information on its own. However, when combined with other information held or available to the APP entity, it may become ‘personal information’.

For example, information associated with a unique identifier assigned by an NFP (such as a donor ID) will be personal information for the NFP, but may not be personal information for other entities that do not have access to the database connecting the unique identifier with that individual’s corresponding personal details.

|  |
| --- |
| **👍 Best practice tip:** If it is unclear whether an individual is ‘reasonably identifiable’, an APP entity should err on the side of caution and treat the information as personal information. |

### Sensitive information

Sensitive information is a subset of personal information that includes information or an opinion about a person’s racial or ethnic origin, political opinion or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health or genetic information, and some aspects of biometric information.

Generally, the Privacy Act applies a higher standard of care (and affords a higher level of protection) for sensitive information.

Name

Contact details

Financial information

Communication records

Donation records

Family information

Photographs

Health information

Criminal record

Sexual orientation or practices

Racial or ethnic origin

Religious beliefs

**Sensitive Information**

**Personal Information**

## Are NFPs required to comply with the Privacy Act?

|  |
| --- |
| **Snapshot**: Whether an NFP will need to comply with the Privacy Act depends on its size and activities. There is no general exemption for the activities of charitable organisations or other NFPs under the Privacy Act (compared to, for example, under spam legislation). |

The Privacy Act generally applies to private sector organisations and Commonwealth government agencies (called ‘**APP entities**’). There are some exemptions from the application of the Privacy Act.

In general, an NFP will be an APP entity if it meets any of the following:

|  |  |
| --- | --- |
| 🗹 | Annual turnover greater than $3 million (that is, not a [small business](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/small-business))  *Annual turnover for the purposes of the Privacy Act includes all income from all sources. It does not include assets held, capital gains or proceeds of capital sales* |
| 🗹 | Provides a health service to a person, even if that service is not its primary activity)  *For example, providing a service to help improve diet or fitness* |
| 🗹 | Buys or sells personal information.  *For example, buying or selling donor lists, providing a donor list in exchange for sponsorship* |
| 🗹 | Contracted service provider for a Commonwealth contract (for example, an aged-care provider or disability services provider)  *For example, providing disability services under a contract with a Commonwealth agency* |
| 🗹 | Opts-in to the Privacy Act |
| 🗹 | Related to a body corporate that meets any of the above criteria, even if the NFP itself does not.  *For example, the NFP’s parent company has an annual turnover of more than $3 million* |

**Further information?** Use the free online tool at oaic.gov.au to assess whether your NFP is an APP entity [insert link].

|  |
| --- |
| **👍 Best practice tip**  Even if your NFP is not required to comply with the Privacy Act, there are benefits in having robust privacy practices in place. It demonstrates the NFP’s commitment to good privacy practices and strengthens its reputation with its donors and the community and can help build and maintain trust. This trust is crucial, especially if the NFP depends on ongoing support from donors, members, volunteers, or the community generally.  It also helps to future-proof operations if the applicability of the Privacy Act to the NFP changes over time. For example, if the NFP grows in size or its activities change, or if there is a change in law. Reforms to the Australian privacy laws expected in 2024 include proposals to expand the scope of organisations that are caught by the Privacy Act by removing the small business exemption. |

### Exemptions under the Privacy Act

Even if an NFP is required to comply with the Privacy Act, there may be exemptions that apply to certain activities and personal information held by the NFP.

Key exemptions that may apply to NFPs include:

### Employee records exemption

The employee records exemption is an exemption under the Privacy Act for the handling of employee personal information held in an employee record that is directly related to a current or former employment relationship between the employer and the employee, subject to some important exceptions.

The employee records exemption **does not apply** in certain circumstances, including:

* the handling of employee tax file numbers (see [ref] below)
* the handling of personal information of non-employees (such as individual contractors or consultants, interns, work experience students, or unsuccessful job applicants)
* the sharing of personal information of an employee with a related body corporate
* where the connection with the employment relationship is not maintained (such as use of employees’ personal information to market a supplier’s products to those employees)
* the initial collection of health or other sensitive information. Consent to the collection is still required and the employee records exemption will only apply once the sensitive information is collected with consent and included in an employee record.

It is also important to remember that handling of employee information is also subject to other laws and regulations, including workplace legislation.

### Commonwealth service provider

If the NFP is only required to comply with the Privacy Act because it is a contracted service provider for a Commonwealth contract, the Privacy Act would only apply to that NFP’s handling of personal information collected or held in relation to that contract.

**Further information?** More information about the employee records exemption and other exemptions under the Privacy Act, including the small business exemption and the related bodies corporate exemption, see the guidance from the OAIC here: [insert link].

## What are the key obligations under the Privacy Act for NFPs?

### Australian Privacy Principles

|  |
| --- |
| **Snapshot**: The APPs govern how NFPs must handle personal information throughout the information lifecycle. They are the foundation of Australia’s privacy laws applicable to personal information. |

The APPs apply to the personal information ‘held’ by APP entities. That is, personal information contained in a record that is within the within the possession or control of the APP entity. A ‘record’ includes a document or electronic or other device but does not include a generally available publication.

The table below sets out a high-level description of key obligations for an NFP under the APPs. This description is not exhaustive of an NFP’s obligations under the Privacy Act.

| **APP** | **Category** | **Obligation for NFPs** |
| --- | --- | --- |
| 1 | **Open and transparent management** | Ensure personal information is managed in an open and transparent way, including by having a clearly expressed published privacy policy. |
| 2 | **Anonymity and pseudonymity** | Provide individuals with the opportunity to not identify themselves or use a pseudonym. Limited exceptions apply. |
| 3 | **Collection of personal information** | Only collect personal information where reasonably necessary for one or more of the NFP’s functions or activities, by lawful and fair means, and directly from the individual (exceptions apply). |
| 4 | **Unsolicited personal information** | Determine if it could have collected the personal information under APP 3, and if not, destroy or deidentify the personal information as soon as reasonably practicable and where reasonable to do so. |
| 5 | **Notification of collection** | Take reasonable steps to notify an individual about the collection of their personal information. There is a prescribed list of matters for inclusion in the notice. This is separate from (and in addition to) the longer form privacy policy required under APP 1. |
| 6 | **Use or disclosure** | Only use or disclose personal information for the purposes for which it was collected. Limited exceptions apply. |
| 7 | **Direct marketing** | Only use and disclose personal information for direct marketing purposes (which includes online targeted advertising) if certain conditions are met. Separate legislation governs spam and outbound telephone calls. |
| 8 | **Cross-border disclosure** | Take reasonable steps to protect personal information before it is disclosed to an overseas recipient. The disclosing entity is responsible for a breach of the APPs by the overseas recipient, unless an exception applies. |
| 9 | **Government related identifiers** | Not adopt government related identifiers (such as drivers licence numbers or Medicare numbers) as its own identifier for individuals or use or disclose a government related identifier of an individual. Limited exceptions apply. |
| 10 | **Data quality** | Take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up to date and complete. |
| 11.1 | **Data security** | Take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. |
| 11.2 | **Data retention** | Take reasonable steps to destroy or de-identify personal information once it is no longer needed, unless required by law or court order to retain. |
| 12 | **Individual rights – access** | If requested by an individual, give that individual access to their personal information within a reasonable period after the request is made (subject to certain exceptions). |
| 13 | **Individual rights – correction** | If requested by an individual, correct the personal information it holds about that individual within a reasonable period after the request is made (subject to certain exceptions). |

### Mandatory data breach notification

|  |
| --- |
| **Snapshot**: **Data breach myths**  Not all data breaches result from a ransomware or other cyber-attack: data breaches include any unauthorised access or disclosure, or loss, of personal information help by your NFP. A data breach could arise, for example, when sending an attachment to the wrong email recipient.  And not all data breaches require notification under the Privacy Act. It is only “eligible data breaches’ that require notification (see below explanation). Your NFP may also have contractual obligations to notify third parties in the event of a cyber incident or other data breach, even where it is not notifiable under the Privacy Act.  Your NFP will need to have a documented process in place to enable your NFP to identify, respond, remediate and recover from a data breach. Make sure you regularly review and update, and train employees, senior management and the Board on, the plan. |

The Privacy Act includes a mandatory data breach reporting regime, known as the Notifiable Data Breaches (**NDB**) scheme.

A data breach occurs where there is unauthorised access to or disclosure of personal information held by an APP entity, or where personal information is lost. Data breaches may be caused by malicious action (by an external or internal party), human error or a failure in information handling practices or security systems.

For example:

* A device containing donor records is lost or stolen.
* A spreadsheet of individual beneficiaries of an NFP is attached to an email and sent to the wrong email recipients.
* The IT system of the NFP’s service provider used to host the NFP’s records, including donor and employee information, is hacked by an unknown third party.

The NDB scheme requires APP entities to notify the OAIC and affected individuals about ‘eligible data breaches’:

|  |  |
| --- | --- |
| 🗹 | The data breach involves unauthorised access to or disclosure of personal information, or personal information is lost in circumstances where unauthorised access or disclosure is likely to occur |
| 🗹 | The data breach is likely to result in serious harm for affected individuals  *For example, where a data breach involves unauthorised access to a charity’s donor database by a threat actor, and the threat actor exfiltrates credit card details and other personal information of donors, there is a risk that such donors could suffer financial loss through fraud as a result of the breach, as well as other privacy harms.* |
| 🗹 | The APP entity is unable to prevent the likely risk of serious harm with remedial action |

An APP entity must conduct a prompt and reasonable assessment if it suspects it may have experienced an eligible data breach, generally to be concluded within 30 days.

If an APP entity fails to comply with its obligations under the NDB scheme, this is an “interference with privacy’ under the Privacy Act and subject to possible enforcement action. This could include the OAIC applying to the Federal Court for civil penalties and/or imitating an investigation or taking other enforcement action.

Where an eligible data breach affects more than one entity (for example, where personal information is in one organisation’s possession, but under the control of another), each entity has obligations under the NDB scheme. However, one of the entities may notify on behalf of the other(s). It is generally recommended to provide for this scenario in contractual arrangements with third party suppliers and partners.

For example, an NFP may engage a telemarketing company to make fundraising calls using a database provided by the NFP, which contains donor personal information (the **list**). The personal information on that list will be considered jointly held as the telemarketing company has possession of it, but it is under the effective control of the NFP. Where there is an eligible data breach involving the list in the possession of the telemarketing company, both the telemarking company and the NFP will have obligations under the NDB scheme. The parties should agree between them which party will notify affected individuals and the OAIC.

**Further information?** See the data breach response guidance provided by the OAIC [insert link].

### Tax File Numbers

|  |
| --- |
| **Snapshot**: Tax File Numbers are regulated under a special (and legally binding) rule under the Privacy Act. This rule protects TFN information and is not subject to the employee records exemptions. TFN information must be handled with an additional level of care given the potential risk of privacy harm for individuals if their TFN information is not protected. |

While employee records are exempt from the requirements of the Privacy Act under most circumstances ([insert link to Exemptions section]), the handling of Tax File Numbers (**TFNs**) must still be in accordance with the Privacy Act.

TFNs must be handled in accordance with a separate set of rules made under the Privacy Act in the *Privacy (Tax File Number) Rule 2015* (**TFN Rule**) which provides legally binding rules for the collection, storage, use and security of TFNs. Under the TFN Rule, a TFN recipient (that is, anyone is possession or control of a record that contains TFN information) must not record, collect, use or disclose TFN information unless permitted under taxation, personal assistance or superannuation law.

The TFN Rule protects the TFN information of individuals only – that is, the TFN Rule does not apply to TFN information relating to other entities, such as corporate entities, partnerships, superannuation funds or trusts.

**Key obligations for NFPs under the TFN Rule**

|  |  |
| --- | --- |
| **Before requesting a TFN** | Ensure the NFP has lawful grounds to request TFN information – identify and confirm the taxation law, personal assistance law or superannuation law which authorises the NFP to request or collect the TFN information. |
| **When requesting an individual’s TFN** | The NFP must take reasonable steps to ensure that:   1. the individual is informed of the following:    * the taxation law, personal assistance law or superannuation law which authorises the TFN recipient to request or collect the TFN information;    * the purpose(s) for which the TFN is requested or collected;    * that declining to quote a TFN is not an offence; and    * the consequences of declining to quote a TFN. 2. the manner of collection does not unreasonably intrude on the individual’s affairs; and 3. only information that is necessary is requested or collected |
| **When retaining TFN information** | Ensure the NFP takes reasonable steps to secure the TFN information. This includes appropriate access permission and controls for any electronic or physical filing systems. |
| **Data retention** | The NFP must take reasonable steps to securely destroy or permanently de-identify TFN information where:   * the TFN is not required to be retained by law; or * the TFN is no longer necessary for a purpose under taxation law, personal assistance law or superannuation law. |

**Further information?** See guidance from the OAIC here [https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/the-privacy-tax-file-number-rule-2015-and-the-protection-of-tax-file-number-information].

### What are the consequences for contravening the Privacy Act?

The OAIC has a range of regulatory enforcement powers under the Privacy Act, including to conduct investigations, require information or documents to be provided, issue infringement notices and make determinations with respect to privacy complaints.

Where there has been a “serious or repeated interference with privacy”, the OAIC may seek civil penalties up to the greater of:

* A$50 million
* three times the value of the benefit obtained from the breach
* 30% of the entity’s adjusted annual turnover.

## A to Z of key concepts under the APPs

### Collection notices

In addition to publishing a privacy policy, an APP entity must take reasonable steps to provide a collection notice to individuals at the time of collection of personal information (or if that is not practicable, as soon as practicable after collection) (APP 5).

The collection notice must include information about:

* the identity and contact details of the APP entity
* the facts and circumstances, including where the APP entity collects the personal information from someone other than the individual
* whether the collection is required or authorised by law
* the purposes of collection
* what happens if the personal information is not collected
* the usual disclosures of personal information of the kind being collected
* information about the APP entity’s privacy policy, including that it contains information about the individual’s right to access and seek correction of their personal information, and the entity’s complaints process
* whether the organisation is likely to disclose personal information to overseas recipients (and if practicable, the countries in which they are located).

### Consent

Consent is not always required under the Privacy Act when handling personal information. For example, consent is generally not required to collect personal information (unless it is sensitive information). Consent is also not required for a use or disclose that is for the primary purpose of collection.

However, consent may be needed to:

* collect sensitive information (such as health information from a donor); and
* use and disclose personal information in certain ways (that is, uses or disclosures that are not otherwise authorised under the APPs), for example where an NFP proposes to use or disclose personal information for a purpose other than the purpose for which it was collected (for example, the NFP proposes to disclose a donor’s personal information to a third party market research agency).

The current guidance of the OAIC as to what constitutes valid consent under the Privacy Act is set out below (not legally binding, but instructive and this reflects current best privacy practice). The proposed reforms to the Privacy Act include codifying this current position in the Privacy Act).

For consent to be valid under the Privacy Act:

* The individual must be adequately informed, including being made aware of the implications of providing or withholding consent.
* The consent must be voluntary. That is, there must be a genuine opportunity for the individual to provide or withhold consent. In this regard, the OAIC cautions against bundling consent for a variety of collections, uses and disclosures of personal information into a single request. Individuals should also generally be permitted to withdraw their consent at any time (using an easy and accessible process) for further use and disclosure from the time consent is withdrawn.
* The consent must be current and specific. That is, consent should ideally be sought at the time of collection and be specific to the intended use, rather than unspecified or potential future uses.
* The individual must have capacity to understand and communicate their consent.

Consent can be express or implied. However, use of opt-out mechanisms to infer consent should be avoided (for example, requiring the individual to untick a pre-ticked box in order to opt-out), particularly for sensitive information.

|  |
| --- |
| **👍 Best practice tips**  Ensure that online privacy settings reflect a privacy-by-default approach. For example, if you use a tick box on an online form to obtain consent, the box should not be pre-ticked.  Written consent is preferable to verbal consent for evidentiary purposes, especially if there are significant privacy risks involved. If it is not possible to obtain written consent, policies should be developed to ensure there are controls around when verbal consent is and is not acceptable, ID verification to ensure the individual giving the consent is who they say they are, and steps for documenting the verbal consent (for example, written file notes of the date, time, location and other relevant circumstances for the consent).  When obtaining consent, NFPs should inform the individual of:   * the period for which the NFP will rely on such consent in the absence of a material change of circumstances; and * how they can withdraw that consent, and the potential implications of withdrawing consent, for example, no longer being able to access the service. |

### Cross border disclosure

The overseas transfer of personal information is primarily regulated under APP 8 and section 16C of the Privacy Act (which is also known as the “accountability provision”). This applies where there is a disclosure of personal information to a person located outside of Australia.

The general rule under the Privacy Act is that, unless an exception applies:

* before an APP entity discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the overseas recipient will handle an individual’s personal information in accordance with the APPs; and
* the APP entity disclosing the personal information remains accountable for any breach of the APPs by the overseas recipient, unless an exception applies.

The most relevant exception for NFPs disclosing personal information to overseas recipients are:

|  |  |
| --- | --- |
| **Equivalent protection to the APPs** | The APP entity reasonably believes that:   * the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a manner at least substantially similar to the APPs; and * there are mechanisms available to any individuals that are the subject of the disclosed personal information, to enforce that law or binding scheme. |
| **Consent of the individual** | The APP entity expressly informs the individual that if they consent, APP 8.1 will not apply to the disclosure, and the individual subsequently consents to the disclosure.  This should only be considered and relied on in limited circumstances. |
| **Permitted general situation** | A permitted general situation under section 16A(1) of the Privacy Act (other than items 4 and 5) applies to the disclosure, for example, the APP entity reasonably believes the disclosure is necessary:   * to prevent a serious threat to life, health or safety and it is not practicable to obtain the individual’s consent. * to take appropriate action in relation to a suspected unlawful activity or misconduct of a serious nature that is being or may be engaged in. * to assist the APP entity to locate a missing person. * for the establishment, exercise or defence of a legal or equitable claim. |

The OAIC has released guidance (not legally binding, but instructive) that it is generally expected that the APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1).

### Data security

Under APP 11.1, an APP entity must take “reasonable steps” to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification of disclosure.

The term ‘holds’ extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, it may include personal information stored or hosted by a third party service provider (for example, a third party that provides data hosting or other cloud services to the NFP), where the NPF retains the right to deal with that information, including to access and amend it, but does not have physical possession of it.

As to what are “reasonable steps” will depend on the nature of the personal information and the APP entity. What is reasonable’ may also change over time. Examples of the steps and strategies to be considered include:

|  |  |  |  |
| --- | --- | --- | --- |
| 🗹 | ICT security, including security standards | 🗹 | Internal practices, procedures and systems |
| 🗹 | Access security – physical and IT access permissions and controls | 🗹 | Governance, culture and training |
| 🗹 | Third party services providers | 🗹 | Physical security |

### Data retention

Data retention-related obligations are primarily found in APP 10 and APP 11.

At a high level, an APP entity must take reasonable steps to:

* ensure personal information it holds is accurate, up to date, complete and relevant (prior to any use or disclosure).
* protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
* destroy or de-identify personal information where it is no longer needed, unless an exception applies.

One of the key exceptions to the requirement to destroy or de-identify personal information is where the entity is required by law or under a court or tribunal order to retain the information.

This means that any policy or schedule for the deletion of personal information must take into account the entity’s obligations under other laws or orders to retain it. For example, it is a criminal offence for an entity to destroy records that may be used as evidence in court proceedings.

### Direct marketing

The conduct of direct marketing in Australia is regulated largely based on the marketing channel used:

* Emails, text messages and other ‘commercial electronic messages’ are regulated under the *Spam Act 2003* (Cth).
* Outbound telesales must comply with restrictions under the *Do Not Call Register Act 2006* (Cth).
* Personal letters and online targeted advertising (and any other direct marketing activities not regulated under the above) must comply with APP 7 of the Privacy Act.
* There are some provisions in the Corporations Act that are also relevant (such as anti-hawking provisions and endorsements).

APP 7 in the Privacy Act sets out requirements for the use and disclosure of personal information for direct marketing purposes. APP 7 does not apply to the extent that the *Spam Act 2003* (Cth), the *Do Not Call Register Act 2006* (Cth), or any other legislation prescribed by the regulations apply.

Under APP 7, “direct marketing” is not defined, but the APP Guidelines provides:

*Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods or services. It can encompass any communication made by or on behalf of an organisation to an individual, including fundraising communications. The communication may occur through a variety of channels, including telephone, SMS, mail, email, social media, and online advertising.[[1]](#footnote-1)*

The requirements for the conduct of direct marketing under APP 7 depend on how the APP entity collected the personal information that will be used to conduct the direct marketing and whether the individual would “reasonably expect” their personal information to be used for direct marketing purposes:

* An NFP may use and disclose personal information for the purposes of direct marketing where it has collected the information from an individual, the individual would reasonably expect their personal information to be used for the purposes of direct marketing and the NFP provides a simple means to opt-out (and the individual has not opted out).
* Where an NFP has collected the personal information from a third party, or from the individual but in circumstances where the individual would not reasonably expect that their personal information will be used for the purposes of direct marketing, then the information may only be used and disclosed for direct marketing purposes where the individual has consented to the use of their information for direct marketing, or where it is impractical to obtain that consent. The NFP must also provide a simple means to opt-out (and the individual has not opted out) and include a prominent statement about how to opt-out in each marketing communication to the individual.

|  |
| --- |
| **Snapshot:** The proposed privacy law reforms include a number of changes to the Privacy Act to address the change in direct marketing practices since the Privacy Act was first enacted and the resulting increase in risk of privacy harm, some of which are “agreed in principle” by the Government. The precise detail of any reforms to direct marketing is not yet known. The proposed reforms include:   * Providing individuals with an unqualified right to opt-out of the use or disclosure of their personal information for direct marketing purposes (as to the current requirement of APP 7 which requires provision of an opt-out mechanism). * A prohibition on direct marketing and targeting to children, and trading in the personal information of children, except where the direct marketing or targeting is “in the best interests of the child”. The Government recognises there will need to be clear guidance to help guide organisations determine what this means (and doesn’t mean). There is not currently this prohibition, or the distinction between personal information of children and adults under the Privacy Act. * A prohibition on direct marketing using some categories of sensitive information (ethnicity, religion, sexuality, health or disability), unless it is for socially beneficial content, and increased transparency requirements about targeting (including use of algorithms and profiling to recommend content). Any direct marketing activities using sensitive information should be handled with caution, whether or not this reform is passed. * Adding a consent requirement for ‘trading’ of personal information, which includes disclosure of personal information for a benefit, service or advantage. For example, reciprocal data sharing/matching, even where not for a fee, would be ‘trading’ in personal information. |

### Privacy policy

An APP entity must have a clearly expressed and up-to-date APP privacy policy about how it manages personal information (APP 1.3).

The privacy policy must include information on the following (APP 1.4):

* the kinds of personal information collected and held by the entity.
* how personal information is collected and held.
* the purposes for which personal information is collected, held, used and disclosed.
* how an individual may access their personal information and seek its correction
* how an individual may complain if the entity breaches the APPs or any registered binding APP code, and how the complaint will be handled
* whether the entity is likely to disclose personal information to overseas recipients (and if practicable, the countries in which they are located).

An APP entity must also take reasonable steps to:

* make the privacy policy available free of charge and in an appropriate format (APP 1.5)
* give the privacy policy to an individual in the form the individual requests (APP 1.6).

### Sensitive information

|  |
| --- |
| **Snapshot**: An APP entity must generally obtain an individual’s consent to collect sensitive information about them. There are some situations where consent is not needed, for example, where an individual, in need of urgent medical treatment, is unable to consent. An APP entity can only use or disclose sensitive information for the primary purpose for which it was collected (limited exceptions apply). |

The Privacy Act generally affords a higher level of protection to sensitive information.

An APP entity may collect sensitive information if both of the following are satisfied:

* the individual consents (expressly or impliedly) to the information being collected; and
* the information is reasonably necessary for the APP entity’s activities.

When sensitive information is collected, the APP entity collecting the information must take reasonable steps to provide a collection notice to the individual.

Generally, sensitive information should not be used for direct marketing purposes, unless the APP entity have obtained (and maintains) appropriate consent from the individual.

# – Privacy in Practice

## Privacy program management

### Information handling practices

There are many benefits to having a robust privacy program. These include assisting your NFP to ensure compliance with its privacy obligations, reduce the risk of a data breach, and promote trust and confidence that your NFP will manage personal information appropriately.

It is also a requirement under APP 1, which requires APP entities to take reasonable steps to implement practices, procedures and systems that ensure the APP entity complies with the APPs and enables the APP entity to deal with privacy inquiries and complaints.

In creating or reviewing the privacy program for your NFP, you should, at a minimum:

|  |  |
| --- | --- |
| 🗹 | Identify privacy obligations that apply to your NFP. |
| 🗹 | Understand what personal information your NFP collects and holds, where it is held, how it is stored and for how long it is needed. |
| 🗹 | Understand what third party services providers or partners are involved in handling personal information of your NFP. |
| 🗹 | Identify the privacy risks for all stakeholders of your NFP, including donors, beneficiaries, employees and volunteers. |
| 🗹 | Review the existing privacy documentation of the NFP, including policies, procedures and training materials. |
| 🗹 | Conduct a gap analysis – Determine if existing practices, procedures and systems (including existing documentation) should be updated or if additional documentation is needed. |
| **👍 Best practice tip:** One practical approach to comply with the APPs (and also adopt best privacy practice) is to embed a ‘privacy by design’ approach. ‘Privacy by design’, seeks to build privacy into the initial stages and design of a project, technology or process and throughout the information lifecycle, rather than attempting to “bolt it on” when a compliance issue later arises. | |

### Privacy management plan

A key tool recommended by the OAIC to help APP entities meet their ongoing compliance obligations under the Privacy Act is to develop and implement a privacy management plan (**PMP**).

The purpose of a PMP is to set out specific, measurable goals and targets that detail how your NFP will implement the following steps in the OAIC’s privacy management framework:

1. **Embed**: a culture of privacy that enables compliance
2. **Establish**: robust and effective privacy practices, procedures and systems
3. **Evaluate**: your privacy practices, procedures and systems to ensure continued effectiveness
4. **Enhance**: your response to privacy issues

**Further information?** The OAIC has published a privacy management plan template: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/privacy-management-plan-template>

### Privacy training

|  |
| --- |
| **👍 Best practice tip:** Provide ‘bite-sized’ learning opportunities on individual privacy topics on a regular basis to supplement broader on-boarding and annual privacy awareness training. |

Privacy training should be provided to anyone who will, or is likely to, collect or handle personal information on your NFP’s behalf. This includes employees, individual contractors and volunteers. The purpose of the training is to ensure that these individuals are aware of your NFP’s privacy policy and procedures, including what to do if they are planning a project which impacts personal information, or they suspect there is a data breach.

Training should be provided during induction or onboarding, and if required, when an individual changes role or takes on additional responsibilities. This should then be supplemented by refreshers at regular intervals (such as annually or quarterly).

## Privacy policy and collection notices

A privacy policy is a document that is generally published on your NFP’s website and informs individuals about your NFP's privacy management practices more broadly. On the other hand, a collection notice is usually provided at the time the personal information is collected and provides an individual information about how your NFP will handle that specific information.

### Privacy policy

Your NFP must have a clearly expressed privacy policy which it makes available free of charge, and in an appropriate form.

In addition to covering certain mandatory topics (see [ref]), the privacy policy should also be relevant, easy to understand, genuinely informative, specific and up-to-date. Below are some tips for achieving this:

|  |  |
| --- | --- |
| **Do’s** | **Don’ts** |
| 🗹 Treat the privacy policy as a document that helps your NFP to develop trust in its information handling practices | 🗶 Treat the privacy policy as a purely legal document to manage legal risk |
| 🗹 Make the privacy policy specific to your NFP’s functions and activities | 🗶 Repeat the APPs |
| 🗹 Consult and seek input from all stakeholders in your NFP | 🗶 Prepare the privacy policy in a vacuum, with input from only the legal, compliance or executive leadership team |
| 🗹 Keep it simple, both in terms of language and format | 🗶 Use overly complicated or technical language |
| 🗹 Focus on what is important to the reader | 🗶 Cover everything in minute detail |
| 🗹 Take a layered approach, such as including collapsible headings or a summary of key matters | 🗶 Present the policy as a big block of text or long PDF document |
| **👍 Best practice tip:** Include a clearly visible link or privacy icon on each page of the NFP’s website which directs users to the privacy policy. | | |

Additionally, your NFP could:

* display the privacy policy on a stand at reception to its premises.
* distribute a printout of the privacy policy on request.
* include details about how to access the privacy policy at the bottom of all correspondence to individuals.
* where your NFP interacts with individuals by telephone, inform them during the telephone call of how the policy may be accessed in a particular form, for example, as part of a recorded message.

### Collection notice

The content that must be covered by a collection notice is set out in [ref].

Collection notices can be provided to individuals in various ways. The appropriate method will depend on how the personal information is being collected by your NFP. For example, if the information is collected:

* via an online form, either displaying the collection notice on the online form or providing a link to it.
* by telephone, explaining the collection notice to the individual at the start of the of the call (for example, by following a template script or using a recorded message).
* from another entity, ensuring that the other entity has notified or made the individual aware of the matters covered by the collection notice on your NFP’s behalf (for example, through an enforceable contractual arrangement).

If, for some reason, your NFP is unable to provide a collection notice at the time of collection, the notice should be provided as soon as practicable after collection. For example, the collection notice could be provided in subsequent emails to the individual, or by directing the individual to the collection notice on your NFP's website.

|  |
| --- |
| **👍 Best practice tip:** Don’t rely on your NFP’s collection notice (or privacy policy) where consent is required to collect health or other sensitive information. Where consent is required, use a consent form or otherwise seek consent (for example, if collecting over the phone, ask for consent prior to collecting the sensitive information). |

**Further information?** See FIA/PFRA Data Explainer, Guide and Self-Assessment Questionnaire: <https://www.dataphoria.com.au/wp-content/uploads/2021/05/FIA-and-PFRA_DataExplainerGuide_Questionnaire_FINAL.pdf>

## Assessing and managing privacy risks

### Privacy Impact Assessments

|  |
| --- |
| **Snapshot:** The purpose of a PIA is to clearly identify privacy issues and risks and provide for how your NFP will manage, minimise or eliminate privacy risks. |

Privacy Impact Assessments (**PIAs**) lie at the heart of privacy best practice. A PIA should be carried out for projects that may present a risk of privacy harm for individuals (and/or present a risk of non-compliance with the APPs for your NFP).

If your NFP wishes to undertake a project that has or may have the potential to pose a privacy risk, consider if a PIA should be undertaken. For example, projects involving sensitive health information or information that may be sensitive in nature but does not strictly fall within the definition of ‘sensitive information’ (such as information about a person’s family life).

Guidance from the OAIC is that a PIA should commence early enough to influence how the project proceeds and should evolve with the project (PIAs are “living and breathing” documents).

Questions that should be asked as part of a PIA include:

|  |  |
| --- | --- |
| 🗹 | What personal information will be collected as part of the activity? |
| 🗹 | What is the lifecycle of the personal information? Map out how the personal information is collected, accessed, stored, used and disclosed. |
| 🗹 | Will this activity be compliant with the APPs? Identify the risks of non-compliance for the NFP. |
| 🗹 | How does this activity need to be executed to be compliant with your NFP’s external privacy policy and internal PMP and other privacy guidelines? |
| 🗹 | What are the potential risks of privacy harm for individuals? |
| 🗹 | What are the mitigation strategies the NFP will need to put in place to remove or control the privacy risks and risks of harm? |
| 🗹 | Who are the stakeholders that need to be consulted? Have they been briefed on their responsibilities to ensure the mitigation strategies are implemented and maintained? |

**Further information?** See Resources for links to the OAIC guide to undertaking a privacy impact assessment, including online learning course.

### Data security

|  |
| --- |
| **Snapshot:** The obligation to “take reasonable steps” to protect personal information held by the NFP from misuse, interference and loss, and from unauthorised access, modification of disclosure. As to what are “reasonable steps” depends on the nature of the personal information and the size of the NFP. |

Your NFP must take reasonable steps to keep the personal information it holds secure. This includes personal information held in the NFP’s physical and electronic systems, and those of its third party service providers (where the personal information remains under the NFP’s control).

The NFP’s obligations under APP 11.1 are not limited to security of IT systems.

The reasonable steps to be taken will depend on the type of personal information held and an assessment of the risks to the security of the personal information held by your NFP. This should include a combination of physical and technical measures. Some examples of steps that can be taken include requiring, at an organisational level, the following:

* ensuring staff are aware of the NFP’s obligations under the Privacy Act, and their role in ensuring the NFP complies with its obligations.
* implementing and maintaining effective information security measures, such as strong passwords to access computer or IT systems.
* using multi-factor authentication (MFA) for all remote access to business IT systems and for all users when performing privileged action or access data warehouses/repositories.
* up-to-date patches and fixes on operating systems, software, browsers and plug-ins, anti-virus and other end point protection. Appropriate data back-up systems and processes.
* a security pass to use the lift or to access the office.
* a ‘swipe-to-print’ pass in order to print documents.
* locks on office doors and filing cabinets containing physical records of personal information.

**Further information?** See guidance provided by the Australian Cyber Security Centre (ACSC) about the “Essential 8” and other information security best practice, including for small businesses. <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cyber-security/small-business-cyber-security-guide>

There are also things that employees and contractors can do in their day-to-day to keep personal information safe and reduce the risk of privacy breaches, such as:

* locking their computer when they leave their desk or laptop unattended.
* picking up printing promptly.
* being careful with emails, including checking any auto-populated “to” field.
* being aware of common cyber threats such as phishing emails and scam phone calls.
* when discussing donation or donor matters, checking who is listening and moving to a private space if needed.
* protecting storage devices.
* keeping desks clean.
* disposing of documents securely.
* not tailgating through secure doors.

**Further information?** See OAIC’s “Guide to Securing Personal Information”: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>

## Direct marketing

|  |
| --- |
| **👍 Best practice tip:** Establish a compliance program to ensure that any direct marketing activities undertaken in Australia are compliant with applicable Australian law. |

Direct marketing is a key activity for most NFPs and it attracts a somewhat complex patchwork of regulation in Australia.

The Privacy Act imposes a number of obligations on direct marketing activities that are not covered by the Spam Act (eg. email, text message campaigns) or the Do Not Call Register Act (outbound telesales). For example, APP 7 applies to direct marketing sent by letter and to targeted online advertising.

It will be important that your NFP has certainty over how personal information that may be used for direct marketing communications was collected as this will determine what compliance steps need to be put in place. Your NFP will also need to ensure that it has a simple means for individuals to opt-out of future direct marketing communications is provided, and that your NFP complies with any opt-out request. If requested, your NFP will also need to be able to tell an individual where you got their personal information from.

**Further information?** See APP Guidelines at Chapter 7 (Direct Marketing).

## Managing personal information of beneficiaries

### Sensitive information

The general rule is that your NFP should only collect sensitive information, including health information, with the individual’s consent, unless an exception applies.

Your NFP should also only collect the minimum information needed (this applies to personal information, including sensitive information).

Sensitive information, including health information, should also only be collected directly from the individual, unless it is not reasonable or practical to do so. For example, in a medical emergency, the individual’s background health information may need to be collected from their relatives.

Another question that is often raised in relation to sensitive health information is whether such information can be used in an emergency, if that use is not the primary purpose for which the health information was originally collected, or directly related to that primary purpose. This is a complicated issue that will depend on the specific circumstances of collection, the purpose of collection, the emergency and the purpose for which the NFP intends to use the health information. If this is a concern for your NFP, we recommend that you obtain legal advice tailored to your specific circumstances.

### Children

|  |
| --- |
| **Snapshot:** Children are particularly vulnerable to privacy harms (as are other vulnerable members of society). Whilst the personal information of children is not currently subject to additional protections, NFPs should take additional care when handling personal information of children.  The proposed Privacy Law Reforms include a number of changes to the Privacy Act to increase the level of protection of children’s personal information. This includes:   * introduction of a definition of a child to include an “an individual who has not reached 18 years of age”. * a “Children’s Online Privacy Code”, similar to codes in the UK and the US. * additional protections for individuals experiencing vulnerability through the development of OAIC guidance. This guidance is expected to update information about capacity and consent and provide a non-exhaustive list of factors that may indicate when an individual is experiencing vulnerability. |

If your NFP intends to portray children in its marketing materials, it will need to follow the same rules for use and disclosure of personal information detailed in this guide.

Currently, the Privacy Act does not specify an age at which individuals can make their own privacy decisions, rather relying on the issue of capacity to consent. Capacity should be assessed on a case-by-case basis. Generally, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what’s being proposed. If not, it may be appropriate for a parent or guardian to consent on their behalf instead.

However, it may not be possible or practical to assess capacity on a case-by-case basis. If that is the case, OAIC guidance is that, as a general rule, an NFP may assume:

* an individual aged 15 or older has capacity, unless there is something to suggest otherwise.
* an individual under the age of 15 does not have capacity to consent.

**Further information?** FIA Practice Note on Fundraising and Younger People https://fia.org.au/fia-code-course-practice-notes/

### Prospective donor research

The general rule is that personal information about an individual must be collected directly from the individual, unless it is ‘unreasonable or impracticable’ to do so. Whether it is ‘unreasonable or impracticable’ will depend on the particular circumstances.

OAIC guidance is that considerations that may be relevant include:

* whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
* the sensitivity of the personal information being collected
* whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
* any privacy risk if the information is collected from another source
* the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

|  |
| --- |
| **👍 Best practice tip**  If an NFP collects personal information directly from a donor and wishes to use that information to conduct prospect research and collect additional personal information about that donor from public sources, such collection would only be permitted if direct collection from the donor is ‘unreasonable or impracticable’ in the circumstances.  Privacy best practice would be to request the further information from the donor directly. If this is not reasonable or practicable, then the NFP should limit the amount of personal information collected through research and follow the OAIC’s above guidance. It will also be important for the NFP to understand that once collected and added to a donor profile, the NFP then has all of its obligations under the APPs with respect to such personal information. This includes consideration of the following:   * A general approach of “data minimisation” should be taken. * The NFP should ensure its data retention schedule and policy provides for review and, where appropriate, deletion, of any collected prospect research data. * The NFP’s privacy policy and collection notices should include a clear description about the NFP’s intention to conduct prospect research so that the donor would reasonably expect personal information about them to be collected directly from such research. This notice should include:   + the fact that the NFP may use personal information collected for conducting prospect research   + the reasons for doing so (for example, to support the NFP’s mission)   + a description of the types of research conducted   + whether third party service providers will be engaged to assist with such research. |

## Engaging third party service providers

When engaging third party service providers who will have access to, host or store personal information held by your NFP, in addition to having appropriate information security protocols in place with the service provider (such as secure means of access, maintaining access and activity logs, access and permission controls etc), your NFP will need to ensure there is a binding contract in place that includes appropriate contractual controls.

This should include a restriction on the transfer of personal information outside Australia (or clauses to address the risks arising in connection with an overseas transfer), and obligations for the service provider to comply with the Privacy Act with respect to personal information handled in connection with the services provided to your NFP.

|  |
| --- |
| **👍 Best practice tip:** **Contracting with service providers and managing supply chain risk**  Privacy best practice (and market practice for outsourced services arrangements) is to include further express obligations with respect to the handling of personal information, including:   * a description of the types of personal information to be accessed and used by the service provider in connection with the services, and a clear contractual obligation to only access and use personal information for this permitted purpose; * a requirement that the service provider complies with the APPs (as appliable to the services provided) in relation to the collection, use, disclosure, storage and destruction or de-identification of the personal information; * a requirement that the service provider return, or delete or de-identify, personal information at any time on request, or at the end of the term of the contract; * clear technical and organisational security measures to be maintained; * either a prohibition on the use of subcontractors without prior consent from your NFP, or a requirement that any subcontractors be subject to similar contract requirements; * the complaint handling process for privacy complaints (i.e. that complaints will be referred to your NFP for handling); and * a requirement for the service provider to immediately notify your NFP of any breach of its privacy obligations, including where there are reasonable grounds to suspect a data breach. The contract should clearly provide for the data breach response process and remedial action. |

[remember that the NFP and its director and officers may also have obligations under the Corporations Act with respect to managing its supply chain risk]

## Overseas transfers

Before your NFP discloses personal information with an overseas recipient (such as a partner charity located overseas), unless an exception applies.

The two main exceptions for NFPs in a fundraising context are:

* your NFP has a reasonable belief that the overseas recipient is subject to a law or binding scheme that protects the personal information in substantially similar way to the APPs and individuals have a mechanism to enforce that protection (this will depend on the jurisdiction to which you disclose personal information); or
* the relevant individuals provide informed consent to the overseas disclosure on the basis APP 8.1 (which sets out the above obligations for your NFP) will not apply to their personal information. You should exercise caution in relying on this exception, as it will expose your NFP to risk if consent is not obtained correctly, may not be consistent with privacy best practice.

|  |
| --- |
| **Snapshot:**  Where your NFP has a related body corporate located overseas, you will still need to consider the application of the overseas transfer requirements under APP 8.  However, the requirements do not apply where the personal information is accessed by the same entity in a different country (for example, accessed from an overseas office of your NFP). |

### When will my organisation ‘disclose’ personal information to an overseas recipient?

Your NFP will disclose personal information where it makes it accessible to others outside your NFP and release the subsequent handling from your effective control.

If your NFP maintains effective control over the handling of personal information (even if it is accessed from overseas), the provision of information may be a “use” rather than a “disclosure” (in which case, the obligation to take reasonable steps to ensure the overseas entity will handle the personal information in accordance with the APPs will not apply). For example, guidance from the OAIC in the APP Guidelines (not legally binding, but instructive) is that a “use” in the context of an outsourced arrangement will require the following:

* a binding contract that requires the provider to only handle personal information for the limited purposes of the contract.
* the contract to require all subcontractors to comply with the same obligations as the provider in relation to personal information.
* the contract to give the entity effective control over how the information is handled by the provider. This includes addressing whether the provider retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

Generally, you should approach an information sharing arrangement on the basis that it will be a “disclosure”, as the circumstances in which the access will be a “use” are relatively limited.

### ‘Reasonable steps’ to ensure the overseas recipient’s compliance with the APPs

The OAIC generally expects that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient to handle the personal information in accordance with the APPs. Guidance from the OAIC is that this may include:

* a description of the types of personal information to be disclosed and the purpose of disclosure;
* a requirement that the recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of the personal information, and to enter similar arrangements with any third parties to whom it discloses personal information;
* the complaint handling process for privacy complaints (i.e. that complaints will be referred to your NFP for handling); and
* a requirement for the service provider to immediately notify your NFP of any breach of its privacy obligations, including where there are reasonable grounds to suspect a data breach. The contract should clearly provide for the data breach response process and remedial action.

|  |
| --- |
| **Caution!** Consider if the overseas transfer is consistent with the purpose for which your NFP collected the information. Remember that your NFP must only disclose personal information for the primary purpose for which it was collected (unless an exception applies) (see [ref]). |

## Dealing with privacy complaints

|  |
| --- |
| **Snapshot:** Privacy complaints should be carefully managed. If a privacy complaint is not resolved to the satisfaction of the complainant within 30 days, the complainant may make a compliant to the OAIC. This could result in conciliation by the OAIC, or an investigation and determination by the OAIC where it is not resolved by the parties. There are also reputational issues associated with mishandling privacy complaints. NFPs should:   * Implement and maintain a clear process (and ensure all staff are aware of the process) for ensuring privacy complaints are properly identified (they can sometimes be bundled into a general complaint or an access request) and responded to within the required timeframe (generally 30 days). * Consider a central and monitored privacy inbox (eg. [privacy@nfp.org.au](mailto:privacy@nfp.org.au)) to ensure proper oversight and management of privacy complaint handling. |

Individuals have a right to lodge a complaint with the OAIC if they think that an NFP has mishandled their personal information. However, the OAIC is prohibited from investigating the complaint unless the individual has first lodged the complaint with the NFP concerned and a period of 30 days has elapsed. This gives the NFP has an opportunity to resolve the complaint directly first. The OAIC will generally not investigate if it considers that an offer was made to achieve a reasonable outcome or where conciliation of the complaint resolves the matter.

If the OAIC proceeds with an investigation, it has broad powers to:

* investigate the complaint, including the right to compel the collection of information from the NFP
* resolve the complaint, which includes the ability to order corrective steps, apologies, compensation and other relevant non-financial options. The OAIC may also decide to seek a civil penalty against the NFP through the Federal Court.

The OAIC has released a helpful checklist setting out the steps you need to take if your NFP receives a complaint about your NFP’s handling of an individual’s personal information.

At a high level, the steps to take include:

* Determine if the personal information involved in the complaint is the complainant’s personal information, and if not, clarify the complainant’s authority to act for the concerned individual.

|  |
| --- |
| **Caution!** If you continue without confirming the complainant has proper authority to act, you risk disclosing personal information and you may be in breach of APP 6 and APP 11. |

* Contact the complainant to confirm receipt of the complaint, provide details of your NFP’s complaints process and when you will contact the complainant again.
* Determine the issue of the complaint and conduct an internal investigation into the complaint.
* Provide a response to the complainant with the outcome of the investigation, including an invitation for the complainant to reply to your response.
* Assess any reply or further information from the complainant.
* Keep a record of the complaint, the investigation and the outcome.
* After the complaint is closed, consider if any changes are required to your NFP’s privacy program, or if additional training is required, in order to avoid similar complaints in the future.

**Further information?** The OAIC’s checklist can be found here: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/handling-privacy-complaints>

Data retention

|  |
| --- |
| **Snapshot**: Your NFP must take reasonable steps to destroy or de-identify personal information when it is no longer needed for any purpose for which the information may be used or disclosed under the APPs, unless an exception applies.  A key exception to this requirement to destroy or de-identify is where the NFP is required by an Australian law or court/tribunal order to retain the personal information. |

A data retention policy is a useful compliance tool for NFPs; it can help NFPs meet both regulatory and operational requirements. The policy should be tailored to an NFP’s specific circumstances and requirements.

While there is no one-size-fits-all approach, a data retention policy generally includes:

* a schedule outlining all the categories of records held by the NFP (whether containing personal information or not)
* the required retention period at law for each category of record and the relevant legislation (this can be different for different categories of records)
* steps to be taken by the NFP to implement the relevant data retention requirement.

### Retention period and bequests

An NFP may retain personal information if it still needs it for the primary purpose for which the information was collected, or a related secondary purpose. Accordingly, whether or not an NFP will be able to retain donor information for the purpose of tracking and managing a bequest will depend on the purpose for which it was originally collected.

For example, if your NFP collects personal information from a donor for the purpose of processing a one-off donation, it would be difficult to argue that it needs to retain that information for a prolonged period for the purpose of tracking and managing a possible bequest from that donor (unless there is another reason for retaining that information. For example, if the NFP knows or suspects that the information may be required as evidence in court proceedings).

Conversely, if the donor submits an intention to donate form or similar to the NFP indicating their intention to include the NFP in their will, then it is more likely to be able to retain that information for a prolonged period of time.

|  |
| --- |
| **👍 Best practice tip:** Include a collection notice in template “intention to donate” forms which notifies the donor of the NFP’s intention to retain that information for a longer period. Also consider what information needs to be retained for this purpose and seek to minimise what personal information is retained. |

### Deleting and de-identifying personal information

The “reasonable steps” required to be taken to destroy or de-identify personal information once it is no longer required will depend on the circumstances, including the sensitivity of personal information, possible consequences for an individual if their information is not destroyed or de-identified, and the practicality (including time and cost) involved in destroying or de-identifying the information (i.e. whether the burden is excessive in all the circumstances).

Personal information is:

* **“destroyed”** when it can no longer be retrieved - this may include, for example, sanitising software on which the information is stored or instructing a third party storage provider to irretrievably destroy the information and taking steps to verify that this has occurred; and
* **“de-identified”** when the information is no longer about an identifiable individual or individual who is reasonably identifiable. If your NFP were to consider de-identifying personal information instead of destroying the information, it should further consider the risk of potential re-identification.

The above destruction and de-identification obligations do not apply in certain circumstances, including if your NFP is required to retain the personal information by another Australian law or court order to retain. For example, other data retention periods may apply to tax file numbers and employee records. This should be considered when developing your data retention plan.

**Further information?** See OAIC’s “Guide to Securing Personal Information”: <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information>

## Data breaches

### Data breach response plan

There is no express requirement under the Privacy Act to implement a data breach response plan. However, the OAIC has expressed that all APP entities should have a data breach response plan. In particular, OAIC guidance notes that a data breach response plan is required for an APP entity to comply with its obligations under APP 1.2 (reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs) and APP 11.1 (reasonable steps to protect the personal information it holds).

OAIC guidance (which, while not legally binding, is indicative of best practice) is that a data breach response plan should cover the following:

* a clear explanation of what constitutes an eligible data breach (explained [ref])
* a breach response strategy, including:
  + strategies for containing and mitigating the breach
  + legal requirements (e.g. notification deadlines) for compliance purposes (see [ref])
  + a communications strategy (e.g. how individuals will be notified, criteria to determine which regulator(s) to notify, and who is responsible for liaising with external stakeholders)
  + the roles and responsibilities of staff
  + a plan for documenting data breach incidents
  + a strategy for post-breach review address data handling weaknesses and to improve breach response).

### What to do if you suspect there is a data breach?

If your NFP is an APP entity and it believes, or suspects a data breach that may be, an eligible data breach, it has obligations under the NDB scheme. This includes carrying out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the circumstances amount to an eligible data breach. It must take all reasonable steps to ensure that this assessment is completed within 30 days after it becomes aware of the potential breach.

If your organisation then becomes aware there are reasonable grounds to believe an eligible data breach has occurred, it must (as soon as practicable), it must notify the OAIC and affected individuals.

**Further information?** Further guidance on the NDB scheme and how to prepare and respond to data breaches is provided by the OAIC [https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act#the-notifiable-data-breaches-ndb-scheme].

## Recommended privacy documentation

The table below sets out the recommended privacy documentation. The rows in pink indicate documents that an APP entity is required to have under the Privacy Act, as a minimum. All other documents are not prescribed, but highly recommended as a means of demonstrating compliance with APP 1.

| **Document** | **Description** | **How to use** |
| --- | --- | --- |
| **Privacy policy** | Describes to third parties how the organisation collects, uses, stores, discloses or otherwise handles personal information. Includes specific minimum requirements, as set out in APP 1.4. | Made available on the NFP’s website |
| **Collection notices** | Provides specific information about the personal information that is being collected. This is more targeted than the privacy policy, but often includes a link to the privacy policy. | Provided or made available at the time of collection. A layered approach may be taken, where your organisation provides a short form collection notice at the time of collection and refers to a full collection notice published on its website for further details. |
| **Privacy management plan** | Internal guide for staff, volunteers and contractors on the NFP’s process for collecting, using, storing, disclosing, or otherwise handling personal information | Provided or made available to staff, volunteers and contractors. |
| **Privacy complaints handling procedure** | Internal guide for staff, volunteers and contractors outlining the procedure for receiving or managing complaints from the public made to or about the NFP or its activities. | Provided or made available to staff, volunteers and contractors. |
| **Privacy impact assessment template** | Template document for staff to complete when undertaking a privacy impact assessment. | Provided or made available to staff, volunteers and contractors. |
| **Data retention plan and schedule** | Describes how an NFP expects its staff, volunteers and contractors to manage data, from creation through to disposal | Provided or made available to staff, volunteers and contractors. This can also be made available externally or as part of an NFP’s privacy policy. |
| **Data breach response plan** | Describes how an NFP will respond if it experiences a data breach incident, or suspects that one has occurred. | Provided or made available to staff, volunteers and contractors. |

# – Resources

## Glossary

| **Abbreviation or term** | **Definition** |
| --- | --- |
| **APPs** | Australian Privacy Principles contained in the Privacy Act. |
| **APP entity** | A private sector organisation or Commonwealth Government agency that is bound by the Privacy Act. |
| **APP Guidelines** | Guidelines published by the OAIC in relation to the APPs, which is available at: <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines>. |
| **Collects** | An APP entity collects personal information only if the APP entity collects the personal information for inclusion in a record or generally available publication. |
| **Contracted service providers** | In relation to an APP entity, a person who is collecting and handling personal information under an arrangement or contract with that entity. |
| **Data breach** | Unauthorised access to, or unauthorised disclosure of, or loss of, personal information. |
| **De-identified** | Personal information is de identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. |
| **Disclosure** | The Privacy Act does not define “disclosure’. However, the APP Guidelines provide that an APP entity discloses personal information when it makes it accessible or visible to others outside the entity, even if that personal information is already known to the recipient. |
| **Eligible data breach** | Defined under the NDB scheme as a data breach that meets the below criteria:   1. there is unauthorised access to, or disclosure of, personal information held by an APP entity, or personal information is lost in circumstances where unauthorised access or disclosure is likely to occur; 2. this is likely to result in serious harm to the affected individuals; and 3. the APP entity has been unable to prevent the likely risk of serious harm with remedial action. |
| **Employee records exemption** | An exemption under the Privacy Act for the handling of employee personal information held in an employee record that is directly related to a current or former employment relationship between the employer and the employee, subject to some important exceptions. |
| **Holds** | An entity holds personal information if the entity has possession or control of a record that contains the personal information. |
| **NDB scheme** | Notifiable Data Breaches scheme set out in Part IIIC of the Privacy Act. |
| **NFP** | In this guide, “NFP” is used as a short form description of Fundraising Institute of Australia (**FIA**) in the not-for-profit (**NFP**) sector who are undertaking fundraising activities |
| **OAIC** | Office of the Australian Information Commissioner |
| **Personal information** | Information or an opinion about an identified individual or individual who is reasonably identifiable, whether or not the information or opinion is true, and whether the information or opinion is recorded in a material form or not. |
| **PMP** | Privacy Management Plan. |
| **Privacy Act** | *Privacy Act 1988* (Cth) |
| **Privacy Act Reform Response** | The Government’s response to the Privacy Act Review Report published on 28 September 2023 and available at: <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report> |
| **Sensitive Information** | 1. Information or an opinion about an individual’s:  * racial or ethnic origin; or * political opinions; or * membership of a political association; or * religious beliefs or affiliations; or * philosophical beliefs; or * membership of a professional or trade association; or * membership of a trade union; or * sexual orientation or practices; or * criminal record;   that is also personal information; or   1. health information about an individual; or 2. genetic information about an individual that is not otherwise health information; or 3. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or 4. biometric templates. |
| **TFN Rule** | *Privacy (Tax File Number) Rule 2015* |
| **Use** | An entity generally uses personal information when it handles and processes the personal information that is within the entity’s effective control. |

## Resources and links

|  |  |
| --- | --- |
| **Description** | **Link** |
| Full text of the Australian Privacy Principles | [insert link] |
| APP Guidelines  The OAIC published guidelines which outline the mandatory requirements of the APPs, how the OAIC interprets the APPs, and matters the OAIC may take into account when exercising its functions and powers under the OAIC. These guidelines are not legally binding, but are instructive. | <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines> |
| OAIC guidance for developing a privacy policy | <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-developing-an-app-privacy-policy> |
| OAIC guide to undertaking a privacy impact assessment, including online learning course. | <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>  <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/e-learning/undertaking-a-privacy-impact-assessment> |
| OAIC guidance on the TFN Rule | <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/the-privacy-tax-file-number-rule-2015-and-the-protection-of-tax-file-number-information> |
| OAIC checklist for handling privacy complaints | <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/handling-privacy-complaints> |

## Contact details

[insert]

**[Back cover]**

1. <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/direct-marketing> [↑](#footnote-ref-1)