Australian Government

Australian Charities and Not-for-profits Commission

Managing people's information and data

Information for charities about collecting, storing and using the information and data they hold about people

Released: March 2017

Charities and information and data

If a charity delivers services, works with clients and partners, employs staff, engages volunteers or has donors or supporters then it is highly likely that it will need to collect information and data about people. This brings important legal and ethical responsibilities.

The responsible persons of a charity (i.e. its governing body, such as the board or committee) need to be aware of the legal requirements of managing people's information and data. They are responsible for the actions of their charity and must ensure it complies with all the relevant laws governing the collection, storage and usage of people's information and data.

Beyond legal requirements, however, there are community expectations about the way a charity manages the information and data of its donors, supporters, staff and volunteers, and the people it helps. Understanding and meeting these expectations is crucial for protecting a charity's reputation and public support for its work. People are becoming increasingly aware of the importance of privacy and information and data protection. The responsible persons of a charity should carefully consider their

processes for managing people's information and data to ensure that they reflect their charity's values and meet the community's reasonable expectations.

This guide provides charities with a broad overview of their responsibilities and the laws that may apply, and practical tips for managing people's information and data responsibly.

Charities need to collect information and data

It is common for charities to collect and store:

- names, addresses and phone numbers
- ages or dates of birth
- email addresses
- bank account or credit card details (for donors)
- signatures
- employment details
- details of service and product purchases and preferences

Some charities, however, may also need to collect much more detailed information and data, such as those contained in health or education records.

Often charities need to collect and store information and data to:

- provide effective services to clients
- maintain membership lists
- manage donor and supporter lists
- co-ordinate and manage volunteers
- send newsletters or updates to donors, supporters and members
- account for activities or expenses, and
- provide supporting evidence when seeking grants or other funding.

A charity should be clear about the purposes for which it is collecting a person's information and data, and should be careful to only collect, store or use the information and data for those purposes. It should also ensure that the person from whom the information and data is being collected has given consent for it to be

collected, stored and used for those purposes – especially when this involves the information and data of the charity's beneficiaries.

Whatever the purposes may be, the responsible persons of a charity should consider the need for the information and data they are collecting about people, and the obligations that come with the collection, storage and use. Importantly, not all information and data is subject to the same laws.

Risks with managing people's information

Collecting, storing and using people's information and data comes with risks. Knowing the risks and taking steps to mitigate them are important elements of good charity governance.

The risks that come with information and data management include:

- inappropriate use or disclosure of a person's information or data
- inadequate processes or training for staff handling people's information or data
- loss of a person's information or data, either physical or digital
- information or data about a person stolen, either physically or digitally
- the policies and practices of external service providers used to manage people's information or data
- failure to comply with applicable laws
- failure of physical management systems
- malicious external cyber-attacks (e.g. hacking or malware)

A charity's reputation is particularly vulnerable to the consequences of failing to mitigate the risks with information and data management. Poorly managing people's information and data, even inadvertently, leaves a charity vulnerable to outcomes which are likely to have a detrimental effect on its reputation and public support. Importantly, management includes the oversight of any external service providers a charity contracts to manage people's information and data. While a charity can outsource this work, it cannot outsource the responsibilities that come with it.

The responsible persons of a charity should be aware of the risks of their particular practices – including any outsourced to an external service provider – and should have processes in place to protect their charity from those risks.

Charity responsibilities and public expectations

The donors, members and supporters of a charity expect it to operate responsibly, honestly and ethically. This includes the way it collects, stores and uses the information and data it holds about people.

The ACNC requires charities to comply with its five Governance Standards. Within these standards, Governance Standard 5 outlines the duties of a charity's responsible persons. This standard requires a charity to ensure its responsible persons act with reasonable care and diligence and that they act honestly and fairly in the best interests of the charity for its charitable purposes. Charities should keep the Governance Standards in mind – particularly Governance Standard 5 – when setting policies and processes for managing people's information and data.

However, simply complying with all the base requirements of the law may not necessarily meet reasonable community expectations of responsible, honest and ethical practice. Aspiring to best practice should be the aim of the responsible persons of registered charities.

Charities rely heavily on public trust and confidence for support. A good relationship with the public and a committed supporter base can take years – even decades – to build, but can take a fraction of that time to fall apart. It is important that a charity's responsible persons consider the public perception of the way it – or the external service providers it has contracted – collects, stores and uses people's information and data. Maintaining public trust, confidence and support is crucial for a charity's work, and good governance practices are the foundation for this.

Legal obligations

There are laws at both the federal and state level that may apply to the way a charity collects, stores and uses information and data about people. The responsible

persons of a charity should be aware of the laws that apply to their charity, and ensure their charity's staff and volunteers follow processes that comply with these laws.

CAUTION:
Privacy laws at both the state and federal levels are complex and can be difficult to follow and apply in practice. If you are unsure about how the law may apply to your charity specifically, please seek professional legal assistance.

State and territory level:

Laws at the state and territory level differ in each jurisdiction and, as such, may apply to the information and data that a charity holds in different ways and bring different requirements. It is up to the responsible persons of a charity to be aware of state or territory laws that apply to their charity.

For a list of laws and other regulatory agencies in state and territory jurisductions, please see the Office of the Australian Information Commissioner website at oaic.gov.au/privacy-law/other-privacy-jurisdictions.

Federal level:

A charity that collects and stores information and data about people may be subject to the federal *Privacy Act 1988* (Cth) (the Privacy Act). The Privacy Act applies to organisations based on several criteria, which may include charities.

Does the Privacy Act apply?

As at February 2017, a charity will need to comply with the Privacy Act if it meets any of the following criteria:

- has an annual turnover of more than $3 million
- provides a health service to a person
- sells or purchases personal information
- is required to comply with the Privacy Act under a contract (e.g. an aged-care provider or a disability services provider under a Commonwealth agreement)
- is related to a body corporate (e.g. it is a subsidiary) that meets any of the above criteria (even if the charity alone does not), or
- has opted in to the Privacy Act (by choosing to comply despite not meeting any of the above criteria).

NOTE: If you are unsure whether your charity meets these criteria, please consider the free resources available on the website of the Office of the Australian Information Commissioner (OAIC) at oaic.gov.au, or seek professional legal assistance.

If a charity meets any of these criteria, it must comply with the Privacy Act and the Australian Privacy Principles contained within. Charities that do not fit any of the criteria, can opt in to comply with the Privacy Act. Opting in to compliance with the Privacy Act may be a good way for a charity to demonstrate its commitment to transparency, accountability and good governance. More information about opting in to the Privacy Act can be found on the OAIC website at oaic.gov.au/privacy-law/privacy-registers/opt-in-register.

The Australian Privacy Principles (APPs) comprise 13 principles that govern how *personal information* – which is information that can be used to identify a person such as a name and address – must be managed. The APPs are outlined in the next section of this guide.

If a charity manages *sensitive information* – which is information about a person's religious, political or philosophical beliefs, membership of associations or trade unions, racial background, sexuality or health – there are stricter provisions within the APPs that also apply.

For guidance on the definitions of *personal*, *sensitive* and *health* information, please see the OAIC website at oaic.gov.au/agencies-and-organisations/app-guidelines/

The 13 Australian Privacy Principles (APPs):

('APP entity' means an organisation that is required to comply with, or has opted in to comply with, the APPs.)

APP 1: Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up-to-date APP privacy policy.

APP 2: Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3: Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4: Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5: Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6: Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7: Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8: Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9: Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government-related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10: Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11: Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12: Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13: Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For more detailed guidance on each of the Australian Privacy Principles, please see the OAIC website at oaic.gov.au/agencies-and-organisations/guides/app-quick-reference-tool/

Overall, the Privacy Act requires organisations to be clear about:

- when it is collecting personal information
- why it is collecting personal information and what it will do with personal information, and
- how people can gain access to the personal information an organisation holds about them and correct that information if required.

The responsible persons of a charity should be aware of all the requirements of the APPs, including those for storing people's information overseas, when considering their charity's processes for information and data management.

What does this mean for charities' direct marketing?

Direct marketing, such as sending mail or emails or making phone calls directly to individuals to promote a charity's services, raise a charity's profile or solicit donations or support, will involve a charity using the information and data it holds about a person.

For charities that are required to comply with, or opt in to comply with, the Privacy Act, it is important that the responsible persons understand Australian Privacy Principle 7 (APP 7), which sets requirements for direct marketing.

For charities that are not required to comply with the Privacy Act, following APP 7 when considering the use of people's information and data for direct marketing is a good idea. Doing so is good practice and sends a message to donors, supporters and the public that the charity manages people's information and data in a responsible way.

In short, APP 7 says that a charity must not use or disclose a person's *personal information* for the purpose of direct marketing unless it satisfies ***all*** of the following criteria:

- the charity collected the information from the person;
- the person would reasonably expect the charity to use or disclose their information and data for the purpose of direct marketing;
- the charity provides a simple means by which the person may easily request to not receive direct marketing communications from the charity; and
- the person has not made a request to not receive direct marketing communications from the charity.

An exception to this principle may apply in instances where a person would not reasonably expect a charity to use their information for direct marketing. In such instances, a charity may still use the person's information for direct marketing purposes, if it meets ***all*** of these criteria:

- the person has given consent for their information to be used for this purpose (or it is impracticable for the charity to obtain the consent);
- the charity provides a simple means by which the person may easily request to not receive direct marketing communications from the charity;
- the charity provides a prominent statement that the person may make such a request each time that it contacts the person for a direct marketing purpose (or the charity otherwise draws the person's attention to this option); and
- the person has not made a request to not receive direct marketing communications from the charity.

These criteria also apply in situations where a charity collects the person's information from a source other than the person in question (for example, if it collects the information from another charity).

Under APP 7, the use of *sensitive information* is treated differently to *personal information*. For a charity to use a person's *sensitive information* for direct marketing purposes, it must first receive the person's direct consent.

Importantly, APP 7 requires a charity to act on a person's request to not receive direct marketing communications. If a charity uses a person's information for direct marketing (or for facilitating direct marketing by other organisations), the person may request:

- to not receive direct marketing communications from the charity
- to not have their information used for the purposes of facilitating direct marketing communications, and
- that the charity provide the source of its information.

Once a charity receives such a request, it must act on the request within a reasonable time period. The OAIC's APP Guidelines indicate that this will usually be no more than 30 days.

Can a charity share donor lists with other charities?

Sharing donor lists can be an effective way for charities to expand the audience to which they communicate, promote their work, and solicit donations and support. However, charities must be careful to ensure that doing so would meet reasonable community expectations.

For a charity thinking about sharing a list of donors, it is important that it considers how its supporters, donors and the community would view a decision to do so. Before sharing information and data about people, a charity's responsible persons should consider:

- whether the charity has stated that it might share the information or data it holds about people

- whether the charity has given people the option to not have their information or data shared
- the type of organisation with which the charity intends to share the information or data it holds about people, and
- the risks that sharing people's information or data may pose for the charity's reputation and its public support.

A charity must be clear about the purposes for which it collects, stores and uses people's information and data. A charity must not share a person's information or data with other charities or organisations unless the person has given consent for the charity to do so, or the person would reasonably expect the charity to do so.

For charities that are required to comply with, or have opted in to comply with, the Privacy Act, the APPs cover such practices.

The requirements for using or disclosing *personal information* are set out in Australian Privacy Principle 6 (APP 6) and it is important that the responsible persons of charities understand this principle. (If a charity uses or discloses personal information for direct marketing purposes, however, APP 7 would apply instead of APP 6.)

The requirements of APP 6 mean, in short, a charity must only use a person's information for the purpose for which it collected the information (the primary purpose), unless it has received consent from the person to do otherwise.

There are exceptions within this principle, though. A charity may use or disclose a person's information for a purpose other than the primary purpose if it meets these criteria:

- the person would reasonably expect the charity to do so, and
- the information is related to the primary purpose (or directly related to the primary purpose for *sensitive information*).

Exceptions also exist for when:

- the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order
- a charity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body, or
- a permitted general situation or a permitted health situation exists.

Even if a charity is not required to comply with the Privacy Act, following this principle is good practice for managing people's information and data. It will ensure that the charity manages the information and data that it holds about people responsibly, honestly and ethically – and in line with reasonable community expectations.

Buying, renting or selling donor lists

Some charities may want to buy or rent access to donor lists to expand their reach, or even sell their own list of donors. Buying, renting and selling lists occurs in the business sector and may provide benefits for charities too. However, it is important that the responsible persons of a charity consider the community expectations of such practices and the risks that they bring.

In keeping consistency with the practices outlined in Australian Privacy Principle 6, a charity that is considering selling its donor list must be sure that the people on the list consented to having their information and data used in this way, or had a reasonable expectation that the charity would do so. (If this is for direct marketing purposes, however, APP 7 would apply instead of APP 6.)

For a charity that is considering buying or renting a list of donors (whether this be from another charity or a list broker), it is important to consider APP 3, which states that "an APP entity must collect personal information only by lawful and fair means". However, it is also important to note that collecting a person's information and data by "lawful and fair means" does not necessarily mean that the charity can be sure that people provided their consent or had a reasonable expectation that their information and data would be used in this way. It is crucial that a charity's

responsible persons are vigilant in conducting due diligence if they are considering buying or renting a list of donors for their own use.

Tips for managing information and data

There are a number of steps that a charity can take to ensure responsible, honest and ethical management of people's information and data.

The following recommended actions are not exhaustive nor a requirement for registration as a charity with the ACNC, but they provide a foundation on which good governance practices for information and data management can be built:

- only collect a person's information and data by lawful and fair means
- do not share or sell people's information and data without their express recorded permission
- be explicitly clear when collecting a person's information and data about the purpose for doing so
- only collect and store the minimal amount of information and data about a person required for a particular purpose
- only store a person's information and data for as long as it is required for the purpose
- securely store people's information and data both physically and digitally
- only disclose a person's information and data for the purpose for which it was collected and stored
- offer people an option to have their information and data changed, corrected or securely removed
- allow people to have access to and correct their information and data
- accurately record and follow people's marketing preferences
- ensure all the staff and volunteers who have access to people's information and data understand the charity's policies and are properly trained
- implement a clear policy and processes for managing people's information and data
- publish publicly, or make available on request, the charity's policy for managing people's information and data

- if using an external provider to manage information and data, ensure its policies and practices meet legal requirements and the expectations of the charity and the community.

A charity should be transparent about the information and data that it collects, stores and uses. It should be open about its practices and be prepared to answer questions from donors, members, supporters and the public about the way it manages people's information and data. If a charity is not prepared to answer questions about and justify its information and data management practices, it is highly unlikely to be meeting community expectations and may also be in breach of its legal obligations.

Tips for developing a policy for managing people's information

Charities should, as a matter of good practice, have a policy that outlines the way they collect, store and use people's information and data. Such a policy will determine the approach that a charity takes to managing information and data, guide the practices of its staff and volunteers, and provide assurances to its donors, supporters and members. It is good practice for a charity to have this freely available on its website.

Charities that are required to comply with the Privacy Act, or those that have opted in to comply with it, must have an APP Privacy Policy which covers the management of personal information.

A policy for managing people's information and data needs to cover the specific needs of a charity and, as such, there is no single general policy that will be appropriate for all charities. Each charity should have a policy that is tailored to fit its own work.

There are, however, some common aspects of a policy that the responsible persons of a charity should consider when developing their own. A charity's policy for managing people's information and data may include:

- examples of the type of information and data about people that the charity collects, stores and uses

- the processes by which the charity collects people's information and data
- the purposes for which the charity collects, stores and uses people's information and data
- how and where the charity securely stores and protects people's information and data (e.g. digital storage managed locally or held on servers overseas)
- an explanation of when the charity will disclose people's information and data, and to whom
- an explanation of how the charity will use people's information and data
- the processes for addressing breaches of privacy or complaints about the charity's management of people's information and data, and
- the conditions on which an individual can access their information and data, and the process by which they can do so.

A policy that governs a charity's collection, storage and usage of people's information and data should be reviewed regularly to ensure it is up to date, relevant and meets the requirements of any applicable laws. All responsible persons, management, staff and volunteers of a charity should be familiar with the processes outlined in the charity's policy.

Taking information management seriously

Responsible management of people's information and data is an important part of maintaining a good reputation for charities. A good relationship with donors, supporters, members and the public is too precious to risk by not having adequate policies and processes to safeguard people's information and data.

Whether a charity is a large multinational organisation with many employees and complex services or a local neighbourhood organisation run by a few volunteers, poor information and data management – internal or by an external service provider – poses real risks to its reputation. Good policies and processes for information and data management which mitigate risks and protect the charity's reputation should be considered important aspects of good governance by the charity's responsible persons.

Compliance with both federal and state laws that govern management of people's information and is essential. For charities that are required to comply with the federal Privacy Act, or for those that have opted in to comply, serious attention needs to be given to the Australian Privacy Principles.

External resources:

Office of the Australian Information Commissioner:

- The Privacy Act presented on the OAIC website: oaic.gov.au/privacy-law/privacy-act
- OAIC 'Opt-in Register': oaic.gov.au/privacy-law/privacy-registers/opt-in-register
- OAIC 'Privacy law – other legislation': oaic.gov.au/privacy-law/other-legislation
- OAIC 'Rights and responsibilities': oaic.gov.au/privacy-law/rights-and-responsibilities

Fundraising Institute of Australia:

- FIA Privacy Compliance Manual (produced in collaboration with Minter Ellison): fia.org.au/pages/privacy-compliance-manual.html

Justice Connect's Not-for-profit Law:

- Not-for-profit Law's fact sheet on privacy: nfplaw.org.au/privacy/

Australian Council for International Development:

- ACID's Code of Conduct: https://acfid.asn.au/code-of-conduct