Privacy Compliance Manual for Charitable Institutions

May 2019

This Manual may only be used by members of Fundraising Institute Australia

MinterEllison

FOREWORD

Fundraising Institute Australia has commissioned MinterEllison to prepare this updated Manual to assist members.

The Privacy Compliance Manual (updated to March 2019) supersedes the Privacy Compliance Manual which was first published in 2014. It contains some changes to reflect amendments to the privacy laws and to improve the Manual generally since it was first prepared.

In particular, it now contains a section on how to respond to data breaches. It is essential for charities to be aware of the impacts and risk from data breaches, that there are substantial penalties for serious or repeated interferences with privacy and that the Information Commissioner has the power to seek enforceable undertakings. This is quite apart from the reputational damage that a charity may suffer if the privacy of an individual is breached.

In conducting their fundraising activities charitable institutions that our members represent, collect and store significant amounts of personal information of donors, potential donors, their clients and other individuals. This information is vital to their operations. Yet, only 38% of individuals surveyed by the Office of the Australian Information Commissioner in 2017 reported that they trust charities to handle their personal information.[1]

The Privacy Act and in particular, the Australian Privacy Principles contained in the Act, place significant obligations on organisations about what personal information they can collect and how they deal with it.

Interference with an individual's privacy can not only attract punitive measures such as fines and a requirement to give enforceable undertakings, it can also result in severe reputational damage. It is therefore imperative that charities are careful to observe their privacy obligations.

This Manual is designed to provide guidelines to charities on how they can deal with personal information.

DISCLAIMER

This Manual is for guidance only. Individual fundraisers may wish to seek specific advice on how to comply with the Privacy Act.

[1] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy survey*, 2017, 8.

TABLE OF CONTENTS

Part 1: Background and overview

1. INTRODUCTION

1.1 The Privacy Act and the Australian Privacy Principles

1.1.1 The *Privacy Act 1988* ('**Privacy Act**') is a Commonwealth Act that regulates the collection, storage, use and disclosure of different types of personal information by:

(a) Commonwealth and Australian Capital Territory government agencies; and

(b) private sector organisations with turnovers of over $3 million.

(together, **'APP Entities')**

1.1.2 An explanation of the types of information covered by the Privacy Act and exemptions from provisions in the Privacy Act, is set out in Section 2.

1.1.3 The Privacy Act has included 13 mandatory Australian Privacy Principles (**APPs**) that charities must comply with when handling personal information.

1.1.4 The APPs set out minimum standards, rights of individuals and obligations of APP Entities in relation to collecting, using, holding, disclosing, accessing and correcting personal information.

1.1.5 The APPs are a principles-based approach to privacy compliance which allows businesses flexibility to develop their own systems, practices and procedures to handle and protect personal information having regard to all the relevant circumstances (including the size and nature of the business, the types and volume of personal information that it collects and what it uses the information for).

1.1.6 The APPs are explained further in Part 2.

1.2 APP Guidelines

1.2.1 The Office of the Australian Information Commissioner (**OAIC**) has published guidelines about the interpretation and operation of the APPs ('**APP Guidelines**'). The APP Guidelines are not binding. This Manual includes commentary on the APP Guidelines where relevant.

1.2.2 The APP Guidelines are available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/

1.3 Enforcement

1.3.1 The Information Commissioner, who heads the OAIC, is responsible for enforcing compliance with the APPs and has functions and enhanced powers to deal with complaints, give guidance and monitor compliance with the APPs.

1.3.2 The Information Commissioner has the power to investigate a charity's privacy compliance either in response to a complaint or on the Commissioner's own initiative. The outcome of an investigation may result in enforcement action being taken, such as a determination (including to pay compensation) or enforceable undertakings which may be published. The Commissioner may also apply to the Federal Court for civil penalty orders of up to $2.1 million for companies for serious and repeated breaches of the APPs.

1.3.3 The OAIC's Regulatory Action Policy (https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/) emphasises the regulator's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with APP Entities to ensure privacy best practice and prevent breaches.

1.3.4 Whether the Information Commissioner will exercise their enforcement powers depends on factors including:

(a) the seriousness of the incident or conduct to be investigated (including the number of people potentially affected and nature of the information);

(b) the level of public interest or concern relating to the conduct, proposal or activity;

(c) whether the entity responsible for the incident or conduct has been the subject of prior compliance or regulatory enforcement action by the OAIC, and the outcome of that action;

(d) whether the conduct is an isolated instance, or whether it indicates a potential systemic issue; and

(e) action taken by the entity to remedy and address the consequences of the conduct, including whether the entity attempted to conceal a contravention or a data breach, and whether the entity cooperated with the OAIC and notified affected individuals if appropriate.

1.3.5 In addition to their obligations under law, charities should remain alert to the Privacy Commissioner's powers to publicise breaches of the Privacy Act in the media.

1.4 Complaints and privacy data breaches

1.4.1 Information about responding to complaints and privacy data breaches is contained in Part 4.

1.5 Specific issues

1.5.1 The following specific issues are discussed in Part 3:

(a) spam and telemarketing;

(b) employee records;

(c) use of patient data;

(d) third party-supplied lists; and

(e) use of social media data.

2. INFORMATION COVERED BY THE PRIVACY ACT AND EXEMPTIONS

2.1 Types of information covered

2.1.1 The following types of information are covered by the Privacy Act:

(a) personal information;

(b) sensitive information; including

(c) health information.

2.2 What is 'personal information'?

2.2.1 Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source.

2.2.2 In other words, if the information or opinion identifies an individual or allows an individual to be identified it will be 'personal information' within the meaning of the Privacy Act. It can range from very detailed information, such as medical records, to other less obvious types of identifying information, such as an email address.

2.2.3 Personal information does not include information that has been properly de-identified so that the individual is no longer identifiable either from the information or from the information when combined with other information reasonably available to the charity. Examples of de-identification techniques include removing identifiers, using pseudonyms and using aggregated data.

2.3 What is 'sensitive information'?

2.3.1 Sensitive information is a type of personal information that is given extra protection and must be treated with additional care. It includes any information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, and criminal record. It also includes health, genetic and biometric information.

2.4 What is 'health information'?

2.4.1 Health information is a subset of sensitive information. It is any information or opinion about the health or disability of an individual, the individual's expressed wishes about the future provision of health services and a health service provided, currently or in the future, to an individual that is also personal information. Health information also includes personal information collected in the course of providing a health service. There are also State and Territory laws that regulate the handling of health information:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic); and

(c) *Health Records (Privacy and Access) Act* 1997 (ACT).

2.5 What is a 'record'?

2.5.1 The Privacy Act regulates personal information contained in a 'record'. A 'record' includes a 'document' or an 'electronic or other device'. This definition is inclusive and therefore covers a wide variety of material which might constitute a record.

2.5.2 A 'document' is defined to include anything on which there is writing, anything from which sounds, images or writings can be reproduced, drawings or photographs.

2.5.3 There are some items which are excluded from the definition of 'record', such as a generally available publication (e.g. a telephone directory), and anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

2.6 Which acts and practices are exempt?

2.6.1 The Privacy Act does exempt certain acts and practices by APP Entities from the scope of the Privacy Act.

2.6.2 The following is a summary only of some key exemptions that may be of relevance to a charity:

Small Business

A charity with an annual turnover of $3 million or less will be deemed to be a 'small business' and will, subject to any exceptions, be exempt from the operation of the Privacy Act. An exception applies where a charity holds both health information (other than in an employee record) and provides a health service. In such a case, the charity will not be considered to be a 'small business'.

Employee records

Certain acts or practices directly relating to employee records are exempt from the scope of the Privacy Act. See Section 16 for more information on the employee records exemption.

Transfers between related companies

A related company or 'related body corporate' is defined under the Corporations Act as either a holding company or subsidiary of another body corporate, or a subsidiary of a holding company of another body corporate.

Essentially, a related company refers to businesses that have a shared controlling interest.

The Privacy Act permits a company that is related to another company to share and transfer personal information (except for sensitive information) without consent without breaching the APPs. However, those related companies must still comply with the APPs when using and handling the shared personal information and must use it for the same primary purpose for which the disclosing body corporate collected it.

Part 2: APPs

3. INTRODUCTION

This Part sets out a detailed commentary on each of the APPs. A summary of the obligations under the APPs is contained at Annexure 1.

4. OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION (APP 1)

4.1 Practices and procedures for open and transparent management of personal information (APP 1.1 and 1.2)

Requirement

4.1.1 The object of this principle is to ensure that a charity manages personal information in an open and transparent way (APP 1.1).

4.1.2 A charity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the charity's functions or activities that:

(a) will ensure that the charity complies with the APPs and a registered APP code (if any) that binds the charity; and

(b) will enable the charity to deal with inquiries or complaints from individuals about its compliance with the APPs or such a code (APP 1.2).

4.1.3 The Privacy Act has an overriding object, which is that APP Entities must manage personal information in an open and transparent way. To achieve this objective, a charity must plan in advance *how* it will handle personal information before it collects and processes it.

4.1.4 This requires the charity to plan in advance how to:

(a) comply with each of the APPs;

(b) respond to complaints and inquiries about its compliance with the APPs; and

(c) take 'such steps that are reasonable in the circumstances' to implement practices, procedures and systems relating to its functions and activities to achieve (a) and (b).

4.1.5 The significance of this principle is three-fold:

(a) this is an overarching requirement;

(b) the Information Commissioner has the power to investigate whether an entity is properly managing personal information, even where there is no breach of an APP; and

(c) if a charity is found to be in breach of another APP, it is quite possible that it will also be found to be in breach of APP 1.

4.1.6 Examples of practices, procedures and systems for compliance with APP 1.2 include:

(a) considering privacy obligations when designing and implementing systems or infrastructure for the collection and handling of personal information;

(b) training and communicating to staff information about the charity's information handling policies and practices;

(c) establishing procedures to receive and respond to requests for access and correction, complaints and other inquiries;

(d) establishing procedures to identify and manage privacy risks and compliance issues.

4.1.7 Attached at Annexure 2 is a Privacy Planning Template intended to assist a charity in assessing the personal information that it currently collects and identifying risks involved.

4.2 Consent

4.2.1 Throughout the APPs there are provisions which require consent to be obtained. It is part of being open and transparent that consent is freely obtained and not hidden in lengthy documents or as part of multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose to which collections, uses and disclosures of their personal information they consent. The APP Guidelines provide that this practice of obtaining bundled consents has the potential to undermine the voluntary nature of the consent.

4.3 Privacy Policy (APP 1.3-1.6)

Requirements

4.3.1 A charity must have a clearly expressed and up-to-date policy about the management of personal information by the charity ('**Privacy Policy**')(APP 1.3).

4.3.2 The Privacy Policy of a charity must contain the following information:

(a) the kinds of information it collects and holds;

(b) how it collects and holds information;

(c) the purposes for which it collects, holds, uses and discloses information;

(d) how an individual may access and seek correction of their information;

(e) how an individual may complain about a breach of the APPs and how the charity will deal with that complaint; and

(f) whether the charity is likely to disclose information overseas and, if so, the countries in which the recipients are likely to be located (if practicable to specify) (APP 1.4).

4.3.3 A charity must take such steps as are reasonable in the circumstances to make its Privacy Policy available free of charge, and in such form as is appropriate. A charity will usually make its Privacy Policy available on its website (APP 1.5).

4.3.4 If a person requests a copy of the Privacy Policy in a particular form, the charity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form (APP 1.6).

4.3.5 The APP Guidelines provide that a 'clearly expressed' Privacy Policy, 'should be easy to understand, easy to navigate, and only include information that is relevant to the management of personal information by the entity'. An 'up-to-date' Privacy Policy should be one that is a 'living document' and is reviewed regularly. It would be sensible to diarise a review at least once every 12 months.

4.3.6 It is important that a Privacy Policy be made widely available (including to employees and contractors).

4.3.7 The matters in APP 1.4 are not exhaustive. The Privacy Policy should contain enough information to describe how the charity manages personal information. For example, the Privacy Policy could also include information about a charity's process for updating its

Privacy Policy, any exemptions under the Privacy Act that apply to the charity and the situations in which a person can deal with the charity without identifying themselves. For other examples of information that may be included in a Privacy Policy see:

(a) section 1.33 of the APP Guidelines (see paragraph 1.2.1 of this Manual); and

(b) the OAIC's Guide to developing an APP privacy policy available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy.

4.3.8 A template Privacy Policy is at Annexure 3 and can be adapted as required by charities.

4.3.9 Before preparing a Privacy Policy, charities should fully understand what information they collect and how, and how they use, store and disclose the information.

5. ANONYMITY AND PSEUDONYMITY (APP 2)

Requirement

5.1.1 Individuals must have the option of not identifying themselves or using a pseudonym when dealing with a charity unless:

(a) the charity is required or authorised by law to deal with individuals who have identified themselves; or

(b) it is impractical to deal with individuals who have not identified themselves.

5.1.2 The Information Commissioner considers that unless there is a good practical or legal reason to require identification, a charity must give people the option to interact anonymously.

5.1.3 Most donors will not be able to make donations anonymously as they require evidence of the donation for tax purposes. However, there may be circumstances when anonymity is appropriate, such as general queries via the charity's website or over the phone.

6. COLLECTION (APPS 3, 4, AND 5)

6.1 Collection of solicited personal (including sensitive) information

6.1.1 The APPs differentiate between 'solicited' information and 'unsolicited' information. 'Solicited information' is information that the charity has asked the individual or a third party to provide. Unsolicited information is information provided to the charity which the charity did not request.

Requirement

6.1.2 A charity must not collect solicited personal information (including sensitive information) unless the information is reasonably necessary for one or more of its functions or activities (APP 3.2).

6.1.3 The Commissioner interprets 'reasonably necessary' in a practical sense: the APP Guidelines provide that it is an objective test, namely, *'whether a person who is properly informed would agree that the use or disclosure is necessary'*. The APP Guidelines state that *'the test must be applied in a practical sense'*: if a charity cannot effectively pursue a legitimate function or activity without collecting personal information, then ordinarily such collection would be deemed to be 'necessary' for one or more of its functions or activities. A charity should not collect information on the 'off-chance' that it will be of some use in the future.

6.1.4 The collection of personal information which is required by law would be deemed as being 'necessary' for one or more of a charity's functions or activities.

6.2 Sensitive information (APP 3.3 and 3.4)

Requirement

6.2.1 In general, a charity must not collect sensitive information about an individual, unless an applicable exception applies. The definition of sensitive information is set out in Paragraph 2.3.1.

6.2.2 The exceptions include where:

(a) the individual has consented;

(b) collection is required by law;

(c) it is unreasonable or impracticable to obtain the individual's consent to the collection and the collection is necessary to prevent or lessen a serious threat to the life or health of any individual; and

(d) other specific circumstances exist for sensitive information which is health information (APP 3.3 and 3.4).

6.2.3 Those charities which are providing health services, for example, will collect sensitive information. In a large number of cases, sensitive information, including health information, will be provided by the individual themselves, in which case it is clear that the charity has consent to collect that information.

6.2.4 The APP Guidelines provide that an 'An APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.' The provision by any individual of sensitive information would usually indicate express consent.

6.2.5 Specific issues around consent arise when information is collected about young people and people who are not capable of understanding for what they are giving consent. These issues

are beyond the scope of this Manual.

6.3 Lawful and fair collection (APP 3.5)

Requirement

6.3.1 A charity must collect personal information:

(a) only by lawful and fair means; and

(b) not in an unreasonably intrusive way.

6.3.2 Under the APP Guidelines, 'fair' means of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive. For example, covert collection will usually be considered as unfair collection.

6.3.3 Examples of what might be considered unfair or unreasonably intrusive ways of collection include:

(a) calling an individual late at night or at meal time without a prior arrangement to do so;

(b) asking for information for one purpose when really it is for another purpose;

(c) telling an individual that it is compulsory that they provide personal information when it is not; and

(d) asking for sensitive personal details within earshot of other people.

6.4 Ensuring the individual is fully aware of collection (APP 5.1)

Requirement

6.4.1 At or before the time (or, if not practicable, as soon as practicable after) a charity collects personal information about an individual, the charity must take such steps (if any) as are reasonable in the circumstances to notify or make the individual aware of such of the following matters that are reasonable in the circumstances:

(a) the charity's identity and contact details;

(b) if the individual may not be aware that the information has been collected, the fact that it has been collected and the circumstances of the collection;

(c) if collected under or authorised by law, the fact that the collection is so required or authorised (including details of the law requiring or authorising collection);

(d) the purposes for which it is collected;

(e) the main consequences if it is not collected;

(f) any other entities or types of entities to whom the information may be disclosed;

(g) that the charity's Privacy Policy contains information about how an individual can access and seek correction of their information;

(h) that the charity's Privacy Policy sets out how an individual may complain about a breach of their privacy and how the complaint may be dealt with; and

(i) whether information is likely to be disclosed overseas and, if so, to which countries, if practicable to specify.

6.4.2 Deciding on whether a charity should make individuals aware of the required matters 'at or before the time of collection' will depend on the circumstances. This can be done after

collection of the information if there are practical problems in doing so before collection. This information should be provided in a collection notice (see 6.4.11).

6.4.3 APP 5.1 has a 'double reasonableness' provision. A charity is only required to take 'reasonable steps' to inform people of such of the required matters that are 'reasonable' in the circumstances. Therefore, it is recognised that where such of those matters are obvious, irrelevant or can be easily located (e.g., the identity of the charity) it may not be necessary to inform people of that matter in a collection statement. The APP Guidelines provide that it is the responsibility of the entity to be able to justify not taking any steps.

6.4.4 In the same way, where the circumstances of collection make a matter listed in APP 5.1 obvious, then the 'reasonable steps' might not involve any active measures because the circumstances speak for themselves. For example, if the matters contained in APP 5.1 were made available to an individual for a certain type of collection, then the same collection later may not require that the APP 5.1 matters (if unchanged) be repeated to the individual.

6.4.5 Deciding what are reasonable steps and what are matters which are reasonable to include involves balancing a number of possible factors, including the importance to the individual of having the relevant knowledge and the time and cost to the charity in providing that information.

6.4.6 The description of the purposes can be reasonably general as long as the description is adequate to ensure that the individual is aware of what is going to be done with their personal information. Internal purposes that form part of normal business practices, such as auditing, business planning or billing do not have to be described.

6.4.7 Taking 'reasonable steps' to inform an individual about usual disclosures would ordinarily mean either giving general descriptions of sets of people and entities to whom the information may be disclosed (for example, other charities) or listing each member of the set.

6.4.8 A charity does not need to mention disclosures that the APPs permit, but in practice happen only rarely.

6.4.9 Reasonable steps must be taken to tell the individual about any law that requires the individual to provide, or the charity to collect, personal information in the particular situation. In describing the law, the charity need not specify the exact piece of legislation (although it would be desirable to do this where possible).

6.4.10 A charity need not describe all possible consequences of not providing personal information. Only significant (and non-obvious) consequences would need to be described.

6.4.11 Privacy collection notices should be given to donors, job applicants, contractors and volunteers, and other individuals from whom the charity collects personal information. The notices should be tailored for each type of collection. For example, the uses and disclosures of donors' information is likely to be very different to the uses and disclosures of volunteers' information.

6.4.12 A common sense and pragmatic approach should be taken when complying with APP 5.1 and APP 5.2. The requirements make it clear that there will be occasions where it is reasonable not to advise people of some or all of the matters set out in APP 5.2. This would be the case, for example, when those matters are obvious or likely to be known.

6.4.13 The APPs provide that personal information should be de-identified or destroyed when it is no longer needed. As such, if charities wish to retain the information of unsuccessful applicants (including contractors and applicants for employment or volunteer opportunities) on file, in case another position becomes available, this should be included in the collection notice.

6.4.14 Annexure 4 contains example privacy collection notices that charities can tailor to their particular activities to comply with APP 5.1 and 5.2.

6.4.15 Where the charity has received personal information from a third party, consideration will need to be given as to whether to provide a collection notice. Often, the most practicable time will be when the charity first corresponds with the individual.

6.5 Collection of information directly from the individual (APP 3.6)

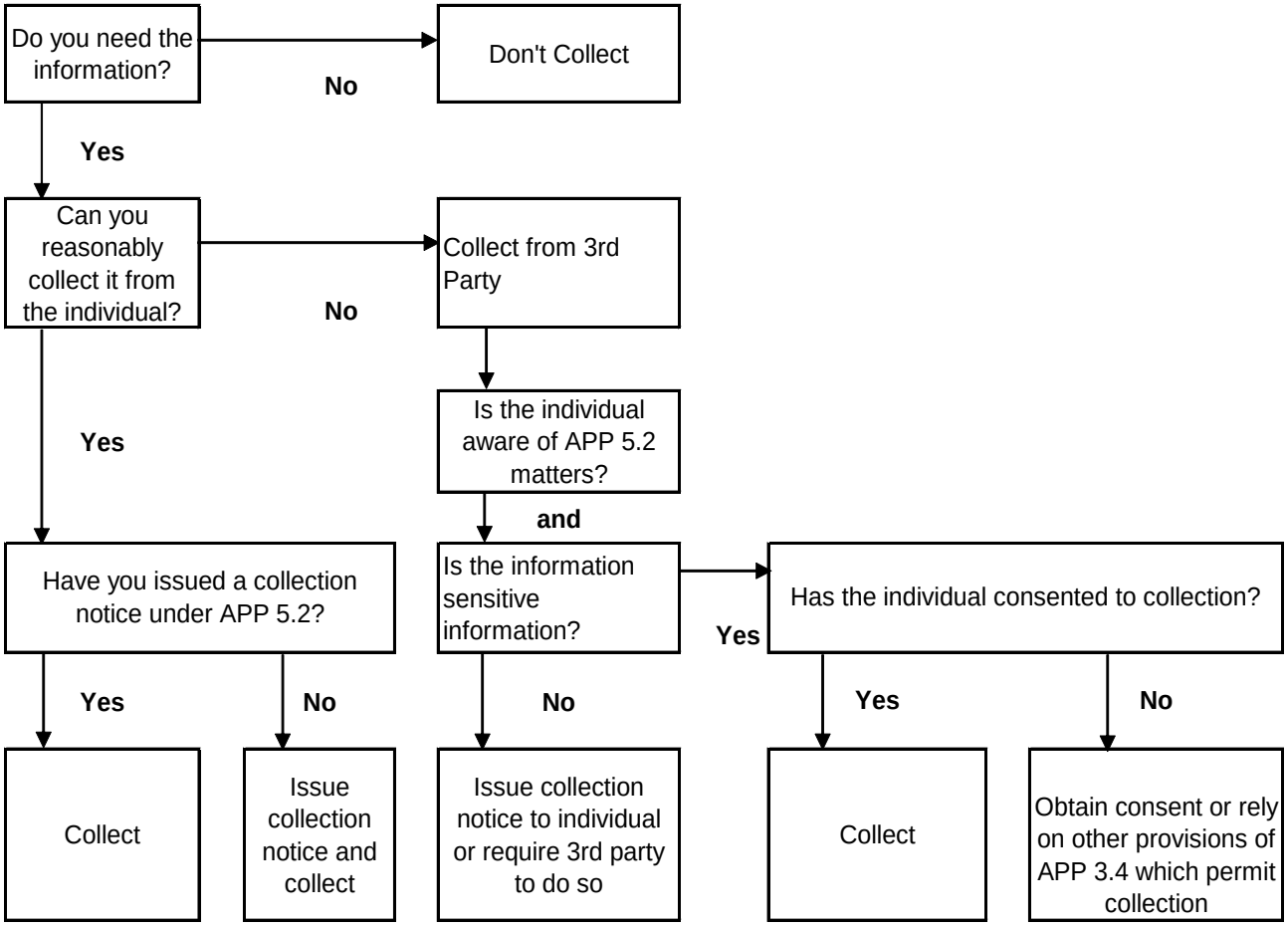
Requirement

6.5.1 Unless consent is obtained, if reasonable and practicable, personal information must only be collected directly from the individual.

6.5.2 APP 3.6 aims to ensure that, where it is reasonable and practicable to do so, a charity will collect information about an individual only from that individual.

6.5.3 It will not always be reasonable and practicable to collect personal information from the individual directly. For example, some charities obtain lists of potential donors from other charities or from public sources.

6.6 Collection compliance steps - Table 4



6.7 Unsolicited personal information (APP 4)

Requirements

6.7.1 If a charity receives unsolicited information it did not request, it must within a reasonable period determine whether it could have collected that information under APP 3.

6.7.2	If it determines that it could not have collected the information under APP 3 it must, if lawful and reasonable to do so, destroy or de-identify the information.

6.7.3 This provision places an obligation on charities to ensure that they only keep information they could have collected. That is, where any unsolicited personal information it receives is reasonably necessary for one or more of the charity's functions or activities. If it is sensitive information and the person has not consented to its collection, it would need to fall within one of the exceptions referred to at Paragraph 6.2.

6.7.4 On occasions unsolicited personal information may be received orally. In order to meet the requirements of APP 4, charities should adopt a rule that any notes of unsolicited personal information received orally should not be made unless it is needed and, in the case of sensitive information, an exception for collection without consent exists.

7. USE OR DISCLOSURE OF PERSONAL INFORMATION (APP 6)

Requirement

7.1.1 A charity must not use or disclose personal information about an individual other than in specified circumstances including:

(a) for the primary purpose for which it was collected (APP 6.1); or

(b) for another secondary purpose:

(i) the individual consents to (APP 6.1(b));

(ii) which is related to the primary purpose of collection (or directly related in the case of sensitive information), and which the individual would reasonably expect (APP 6.2(a));

(iii) which is required or authorised by or under law (APP 6.2(b));

(iv) which the charity reasonably believes is necessary to prevent serious threats to life, health or public safety (APP 6.2(c));

(v) if the charity has reason to suspect that unlawful activity or misconduct of a serious nature relating to its functions or activities has been engaged in and the use or disclosure is necessary in order for it to take appropriate action (APP 6.2(c));

(vi) if the charity reasonably believes it is reasonably necessary to assist with locating a person reported as missing (APP 6.2(c)).

7.1.2 Where a charity collects personal information directly from an individual, the context in which the individual gives the information to the charity will help identify the primary purpose of collection. For example, the 'primary' purpose of collection of donors' information is to receive and process their donation, even if the charity has some additional purposes in mind.

7.1.3 How broadly a charity can describe the primary purpose will need to be determined on a case-by-case basis and will depend on the circumstances. It is likely that in the vast majority of cases the primary purpose of collection will be to enable the charity to process donations. However, this will not be the case with others, such as employees, volunteers, contractors and individuals who the charity assists (if applicable).

7.1.4 Where a charity collects personal information indirectly, a guide to its primary purpose of collection could be what the charity does with the information soon after it first receives it.

7.1.5 *Related and directly related purposes within reasonable expectations*
A charity can also use and disclose the personal information for a related or, for sensitive information, directly related purpose where the individual has a reasonable expectation of that use or disclosure. To be related, the secondary purpose must be something that arises in the context of the primary purpose.

For sensitive information the use or disclosure must be directly related to the primary purpose of collection. This means that there must be a stronger connection between the use or disclosure and the primary purpose of collection.
By way of example, if an employee of a charity seeks assistance in a personal matter from one of the charity's publicly available services, the charity should not inform the employee's supervisors of their application for assistance as this use is not related to the primary purpose of collection (see *C v Charity* [2011] PrivCmrA 3).

7.1.6 *Reasonable expectation*

The test for what the individual would 'reasonably expect' would be applied from the point of view of what an individual with no special knowledge of the industry or activity involved would expect. The APP Guidelines provide that the 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the APP Entity to be able to justify its conduct.

Including the purposes for which an individual's information may be used or disclosed in the charity's Privacy Policy and the collection notice provided to the individual under APP 5 is a good tool to assist in raising a reasonable expectation of such uses and disclosures.

7.1.7 *Factors to consider*

When thinking about whether a use or disclosure falls within the primary purpose or a related or directly related secondary purpose within the individual's reasonable expectations a charity could, where relevant, consider:

(a) the context in which it is collecting the personal information;

(b) the reasonable expectations of the individual whose information it is;

(c) the form and content of information the charity has given about why it is collecting the individual's information (for example under APP 1.4 and 5.2); and

(d) how personal, confidential or sensitive the information is.

7.1.8 *Secondary use and disclosure with consent (APP 6.1(a))*

A charity may use or disclose personal information for a secondary purpose if it has the individual's consent. Consent to the use or disclosure can be express or implied. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the charity.

If the charity's use or disclosure has serious consequences for the individual, the charity would have to be able to show that the individual could have been expected to understand what was going to happen to information about them and gave their consent. In such situations it would ordinarily be more appropriate for the charity to seek express consent.

7.1.9 *Disclosure of donors' names*

It is not uncommon for charities to share lists of donors. This involves a disclosure of personal information, and it may (although it is not beyond argument) be a related secondary purpose to the purpose of collection. However, it is unlikely that it would be reasonably expected unless donors had been told this would occur in such a way that it is clearly drawn to their attention. Some charities seek specific consent to disclose names to other charities.

Another form of disclosure is to publicly acknowledge donations. Again, this is a related secondary purpose but is not necessarily expected. It is suggested that specific consent should be sought to publicise a donation or donors are clearly advised that the donation will be publicly acknowledged unless they advise otherwise.

8. DIRECT MARKETING (APP 7)

Requirements

8.1.1 A charity must not use or disclose personal information it holds for the purpose of direct marketing, unless:

Scenario 1:

(a) it collects the information from the individual;

(b) the individual would reasonably expect the charity to use or disclose the information for direct marketing; and

(c) there is a simple means by which the individual can request not to receive direct marketing from the charity, of which the individual has not availed him or herself (APP 7.2).

Scenario 2:

(a) either:

(i) it collects the information from the individual and the individual would not reasonably expect the charity to use or disclose the information for direct marketing; or

(ii) the information is collected from a third party; and

(b) either:

(i) the individual has consented; or

(ii) it is impracticable to obtain consent; and

(c) there is a simple means by which the individual can request not to receive direct marketing from the charity; each direct marketing communication contains a prominent statement that the individual may request not to receive such communications; and the individual has not availed him or herself of this (APP 7.3).

8.1.2 If a charity uses or discloses personal information for the purpose of direct marketing the relevant individual may request:

(a) not to receive direct marketing communications;

(b) that their personal information not be used by or disclosed to other entities for the purpose of facilitating direct marketing; and

(c) to be provided with the charity's source of the information (unless it is impracticable or unreasonable to do so).

8.1.3 Sensitive information may not be used or disclosed for the purpose of direct marketing unless the individual has consented (APP 7.4).

8.1.4 Instruments such as the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth) will displace the requirements of APP 7 (APP 7.8).

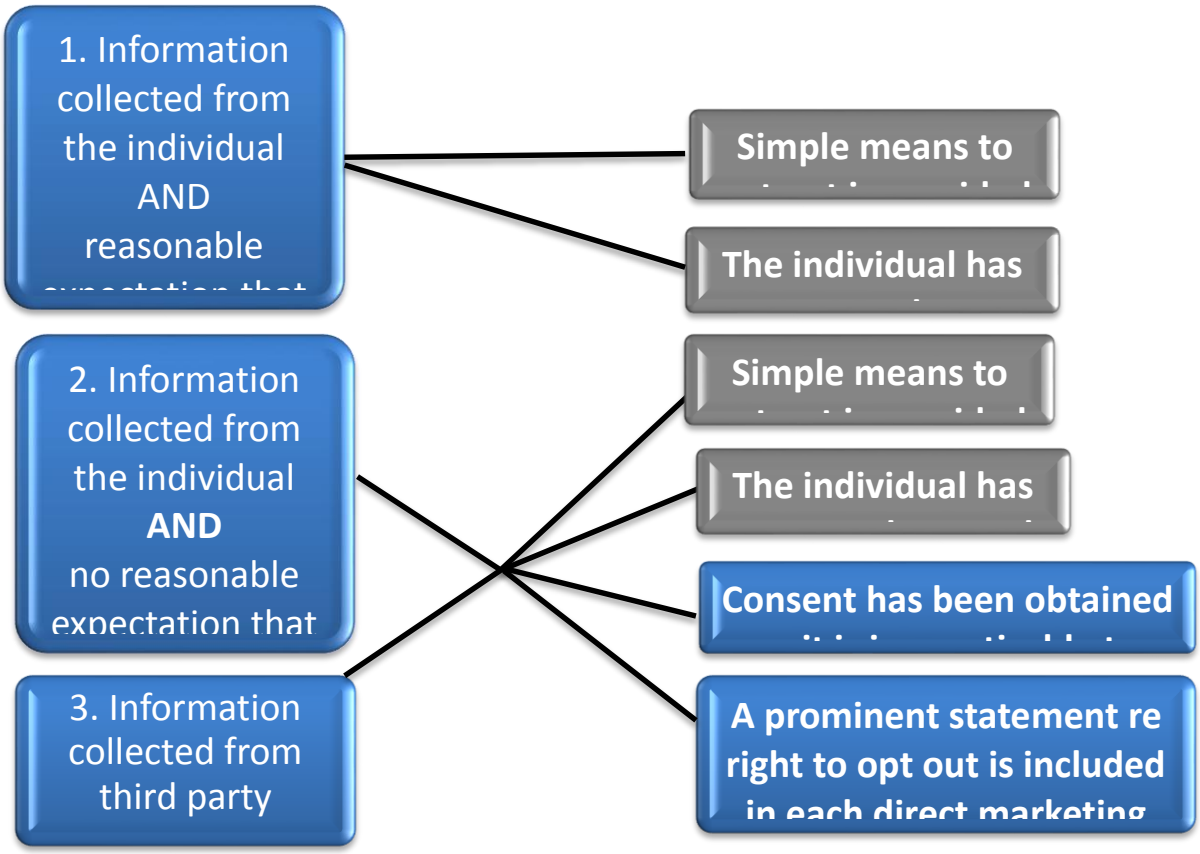
8.1.5 'Direct marketing' involves the use and/or disclosure of personal information by a charity to communicate directly with a person to promote goods and services. While it is not beyond argument, it is likely that soliciting the public for donations is likely to involve the promotion of services provided by the charity and constitute direct marketing. In the OAIC's Privacy Business Resource 19: Direct Marketing, the OAIC states that direct marketing can encompass fundraising communications.

8.1.6 The direct marketing communication could be delivered by a range of methods including

mail, telephone, email or SMS. A campaign to obtain donations directly from particular individuals is an example of a direct marketing campaign by a charity.

8.1.7 APP 7 distinguishes between individuals who have been in contact with a charity (such as existing donors) and those who have not. The intention is to apply more stringent obligations when using personal information of individuals who have no pre-existing relationship with a charity, as those individuals would be less likely to expect their information to be used or disclosed for direct marketing purposes.

8.1.8 The diagram below can be used by charities in determining whether they can use an individual's personal information (aside from sensitive information) for direct marketing, and the steps they must take if they can. A charity may not use sensitive information for direct marketing unless it has obtained consent to do so.



8.2 'Reasonable expectation'

8.2.1 Considering whether an individual has a 'reasonable expectation' that their personal information may be used for direct marketing involves balancing a number of factors that could include:

(a) the content of the collection notice provided to the individual;

(b) the way the charity communicates with the individual;

(c) the previous types of communications between the charity and the individual;

(d) how often the charity is in contact with the individual; and

(e) the duration of the charity's relationship with the individual.

The question of 'reasonableness' would generally be considered at the time of the proposed use of the personal information for direct marketing – not the time the personal information was collected.

8.3 Consent

8.3.1 The APP Guidelines state that whether it is 'impracticable' to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, a charity is not excused from obtaining consent by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it impracticable to obtain consent will depend on whether the burden is excessive in all the circumstances.

8.3.2 The APP Guidelines provide that an organisation may obtain the consent from the individual in relation to a subsequent use or disclosure of the individual's personal information for the purpose of direct marketing at the time it collects the personal information. In order to rely on this consent, the charity must be satisfied that it is still current at the time of the use or disclosure.

8.3.3 Where an individual's name is obtained from a list which has been purchased by the charity, the appropriate course would be to include a prominent statement in the first communication to the individual that he or she can opt out of receiving further direct marketing communications, and provide a simple means to do so.

8.4 Spam and telemarketing

8.4.1 APP 7 does not apply to the extent that the *Spam Act 2003* (Cth) or *Do Not Call Register Act 2006* (Cth) apply. The interaction of these Acts with APP 7 is considered in Section 15**.**

9. CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION (APP 8)

Requirement

9.1.1 If a charity discloses the personal information of an individual to a person outside Australia (other than internally or to the individual themselves) it must take reasonable steps to ensure that the overseas recipient does not breach the APPs. It may, however, be held liable for any acts done or practices engaged in by the overseas recipient which are found to be a breach of the APPs. A charity will not be required to comply with this provision in some limited circumstances, including where:

(a) the charity reasonably believes that the overseas recipient is bound by privacy laws which are substantially similar to the APPs **AND** there are mechanisms which the individual can take to enforce those laws (the 'Reasonable Belief Defence'); or

(b) the individual consents to the disclosure having been expressly informed that the overseas recipient may not be required to provide the same protections as are provided by the APPs; or

(c) the disclosure is required or authorised by law.

9.1.2 The provisions of APP 8 will be triggered where a charity chooses to disclose personal information to an overseas recipient. For example, this could occur where a charity in Australia:

(a) liaises with a charity located overseas;

(b) liaises with overseas companies; or

(c) outsources data handling functions to a third party, including 'cloud' service providers.

9.1.3 A number of charities are now storing personal information in the 'cloud'. Cloud providers may be storing the information offshore, sometimes in multiple or changing locations. It is important that charities are aware of the practices of the cloud provider and enter into appropriate arrangements to limit their exposure should a data breach occur. The use of a cloud service provider by a charity may trigger the requirements under APP 8. However, the APP Guidelines provide that where a charity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the charity may access the personal information, the provision of the information will be a 'use' and not a 'disclosure' (and therefore APP 8 will not apply) where:

(a) the contract between the charity and the overseas cloud service provider binds the provider not to use or disclose the personal information except for these limited purposes;

(b) the contract requires any sub-contractors to agree to the same obligations; and

(c) the contract between the charity and the cloud service provider gives the charity effective control of the information.

9.1.4 As this interpretation in the APP Guidelines has been questioned by some, there is still a reference to using an offshore cloud service for storage in the template collection notices.

9.1.5 If a charity is using an offshore cloud service for **more** than storing personal information, the charity will be required to advise people in the charity's Privacy Policy and collection notices that their personal information may be sent offshore and, if known, to which countries.

9.1.6 In circumstances where personal information is likely to be disclosed overseas, the charity

disclosing the information must have procedures in place for ensuring that requirements contained in APP 8 are met.

9.1.7 Compliance with APP 8 can be achieved if the charity:

(a) enters into a contract with each intended recipient of the information which requires the recipient (and any subcontractors) to agree that the information will be dealt with in a manner that complies with the APPs (NB local liability for breaches of the APPs by overseas recipients); or

(b) reasonably believes that the recipient of the information is subject to a law or a binding scheme which provides similar protection to the APPs and which the individual can enforce. This would be achieved, for example, where personal information is disclosed to an organisation situated in a member country of the EU as they have privacy laws offering similar protection to those contained in the APPs; or

(c) obtains a consent from the individual to the disclosure, after telling the individual that the protections provided under the APPs may not apply. The nature of the consent will have to be specifically drafted to meet the particular situation. If charities wish to rely upon this exception they should seek specific advice on the form of notice.

9.1.8 It is strongly suggested that if a charity enters into a contract with a recipient of personal information such as a 'cloud' provider, as well as seeking undertakings to protect the information they should also seek an indemnity from the recipient to protect the charity against claims in the event of a data breach.

10. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS (APP 9)

Requirement

10.1.1 Government related identifiers cannot be:

(a) adopted by a charity as its own identifier to identify an individual unless required or authorised by law; and

(b) used or disclosed by a charity unless it is reasonably necessary to verify identification of the individual or to fulfil its obligations to an agency or State or Territory authority (APP 9).

10.1.2 A government related identifier is a unique combination of letters and numbers, such as a Medicare number or driver's licence number, which government agencies, authorities or contracted service providers allot to an individual.

10.1.3 APP 9 seeks to ensure that increasing use of government identification does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of the data.

10.1.4 Specific tax file number legislation already restricts the way an organisation can collect, use or disclose a TFN.

10.1.5 Charities should ensure that staff do not enter a person's Medicare number, driver's licence number, TFN or other government related identifier, into a database in order to retrieve their record.

11. DATA QUALITY (APP 10)

Requirement

11.1.1 A charity must take reasonable steps to ensure that personal information it:

(a) collects is accurate, complete and up to date; and

(b) uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

11.1.2 The aim of APP 10 is to prevent adverse consequences for people that might result from a charity collecting, using, or disclosing inaccurate, incomplete or out-of-date personal information.

11.1.3 The APPs require that information used or disclosed must be relevant to the purpose for which it is to be used or disclosed. If the purpose of disclosure is not clear this may require a charity to inquire about the purpose before making the disclosure.

11.1.4 Reasonable steps to confirm the accuracy, completeness and currency of the personal information a charity collects only needs to be taken at the time it collects, uses or discloses the information. It is important that information is checked at times it is to be used or disclosed to determine if it is not accurate, complete, up to date or relevant.

11.1.5 A charity should establish procedures for updating records, passing on changes, deleting records that are no longer used or required and contacting entities to which the records have been disclosed.

11.1.6 The reasonableness of the measures taken would depend on:

(a) whether the information is the type that would change over time;

(b) how recently the information was collected;

(c) the reliability of the information; and

(d) who provided the information.

11.1.7 Where personal information is shared between charities, the disclosing and receiving charity should keep records as to whom the personal information was disclosed to/collected from. Once either charity becomes aware of any change in the personal information then that charity should then pass on such changes and corrections to the other charity. This will help ensure that the information held by both charities is consistent and remains accurate and up to date.

12. DATA SECURITY (APP 11)

12.1 Security of Personal Information (APP 11.1)

Requirement

12.1.1 A charity must take reasonable steps to protect personal information it holds from misuse, interference, loss and unauthorised access, modification or disclosure.

12.1.2 The level of security should be in proportion to the risk to the individual if their personal information is not secured. Therefore, extra care must be taken to ensure that very confidential information is particularly secure. People generally expect that their financial information and sensitive information (particularly health information) will be afforded a high level of protection.

12.1.3 When considering the security of personal information, charities must consider all aspects of security, including physical security, logical security, access and use management, and the practices of internet and/or 'cloud' services providers.

12.1.4 It is particularly important that charities restrict which employees, volunteers and contractors can access sensitive information.

12.1.5 Security procedures should be regularly monitored and audited for compliance to ensure their effectiveness. If a privacy security breach occurs, immediate steps should be taken to prevent a repetition of the circumstances giving rise to the breach. Information on handling privacy security breaches is contained in Part 4.

12.1.6 The Office of the Australian Information Commissioner issued a Guide to Securing Personal Information (the **'Security Guide'**) in January 2015, which can be accessed at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information.

12.1.7 The Security Guide indicates that some relevant factors in determining what are 'reasonable steps' could include:

(a) the nature and quantity of personal information held;

(b) the risk to the individuals concerned if the personal information is not secured;

(c) the data handling practices of the charity holding the information; and

(d) the ease with which a security measure can be implemented.

12.2 Destruction and permanent de-identification (APP 11.2)

Requirement

12.2.1 Where personal information is no longer required for an authorised purpose, a charity must take reasonable steps to destroy or permanently de-identify the personal information.

12.2.2 A charity should have in place systems for destroying or de-identifying personal information that is no longer needed.

12.2.3 In determining whether information is no longer required under APP 11.2, the charity should have regard to a number of matters, including:

(a) whether there is a legal requirement to retain the information;

(b) whether it is likely that the information will be required at a later date; and

(c) whether destroying the information would likely have a prejudicial effect on the charity's operations.

12.2.4 If there is a conversion of information collected from hard-copy records to electronic

databases, it is important to consider whether it is possible and appropriate to destroy or permanently de-identify the information in the hard-copy record as soon as practicable after it is processed into the electronic form. In some cases this may be inappropriate.

12.2.5 In cases where it is considered necessary to retain information that is old or superseded, steps must be taken to ensure that this old or inaccurate information is not confused with the new, up-to-date, accurate information. This is especially so where the information concerned is sensitive information and the consequence of relying on the old or incorrect information is adverse or detrimental to, or embarrassing for, the individual.

12.2.6 Destruction of records containing personal information should be by secure means. Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction and should only be used for documents that are already in the public domain. Reasonable steps to destroy paper documents that contain personal information include shredding, pulping or disintegration of paper.

12.2.7 The reasonableness of steps taken to destroy personal information contained in electronic records will depend on the medium within which the data is stored and the available methods for erasing data.

12.2.8 The APP Guidelines provide that where it is not possible to irretrievably destroy personal information held in an electronic format, reasonable steps to destroy it would include putting the personal information beyond use. This means that the organisation is unable to use or disclose the personal information; cannot give any other entity access to it; surrounds it with appropriate technical and organisational security; and commits to take reasonable steps to irretrievably destroy it if, or when, this becomes possible.

13. ACCESS TO PERSONAL INFORMATION (APP 12)

Requirements

13.1.1 A charity must, on request, provide the individual with access to his or her own personal information.

13.1.2 However, there are some exceptions, including where:

(a) the charity reasonably believes that providing access would pose a serious threat to the life, health or safety of any individual, or to public health or safety (APP 12.3(a));

(b) this would unreasonably impact on the privacy of other individuals (APP 12.3(b));

(c) the request is frivolous or vexatious (APP 12.3(c));

(d) the information relates to existing or anticipated legal proceedings between the parties, and the information would not be accessible through discovery (APP 12.3(d));

(e) access would reveal the intentions of the charity in relation to negotiations with the individual in such a way as to prejudice those negotiations (APP 12.3(e));

(f) this would be unlawful (APP 12.3(f));

(g) denying access is required or authorised by or under law (APP 12.3(g));

(h) the charity has reason to suspect that unlawful activity or misconduct of a serious nature that relates to its functions or activities has been engaged in, and giving access would be likely to prejudice the taking of appropriate action in relation to the matter (APP 12.3(h));

(i) providing access is likely to prejudice enforcement related activities conducted by or on behalf of an enforcement body (APP 12.3(i)); and

(j) providing access is likely to reveal evaluative information generated within the charity in connection with commercially sensitive decision-making processes (12.3(j)).

13.1.3 The charity must respond to the request within a reasonable period after the request is made, and give access to the information in the manner requested by the individual where it is reasonable and practicable to do so (APP 12.4).

13.1.4 Where access is denied, the charity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the charity and the individual (APP 12.5). This may mean deleting the information that should not be accessed but otherwise releasing the documents.

13.1.5 Where access is desired, the charity may consider whether the use of mutually agreed intermediaries would allow sufficient access (APP 12.6).

13.1.6 The charity must not charge excessive fees for providing access (APP 12.8).

13.1.7 Where access is denied, the charity must give written notice of the reasons for refusal (except where unreasonable to set that out) and the mechanisms available to complain about the refusal (APP 12.9).

13.1.8 Charities should establish a standard procedure whereby individuals are permitted to access their records except where an exception to the access principle applies. The procedure should also enable the charity to deal with complaints about its compliance with the access provisions.

13.1.9 The charity is entitled to make a charge for providing access on a cost recovery basis (but not for the making of the access request).

13.1.10 The APP Guidelines provide that access can be achieved by:

(a) providing the individual with a copy of the information;

(b) deleting any personal information for which there is a ground for refusing access and giving the redacted version to the individual;

(c) giving a summary of the requested personal information to the individual;

(d) giving access to the requested personal information in an alternative format;

(e) facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes;

(f) facilitating access to the requested personal information through a mutually agreed intermediary.

13.1.11 APP 12 only gives individuals the right to access personal information which the charity holds about that individual. A charity should take adequate steps to verify the identity of the individual requesting access. This may include verifying that an individual has been given authority to access personal information on behalf of another individual. Such steps are likely to vary on a case-by-case basis.

13.1.12 *Unreasonable impact on the privacy of others*

Information that could have an unreasonable impact on another person's privacy can include more than information such as name and address. It could include any information from which the identity of the person could be reasonably ascertained.

13.1.13 *Frivolous or vexatious requests*

Frivolous and vexatious requests could include those that are:

(a) trivial and made for amusement's sake;

(b) made as a means of pursuing some unrelated grievance against the organisation; or

(c) repeated requests for access to the same personal information.

13.1.14 *Access would be unlawful or denial of access is required or authorised by law*

Providing access to personal information would be considered to be unlawful where it would constitute a breach of confidence under the law. Denial of access may be required or authorised by a State, Territory or Commonwealth law, or the common law. If a charity is required by a law to refuse access it must refuse access. If a charity is authorised by law to refuse access it means it may decide whether to provide or refuse access.

13.1.15 *Reasons for denying access*

APP 12 requires that charities must provide written reasons for denial of access and the mechanisms available to complain about the refusal. The reasons may be framed so as not to defeat the purpose of denying access (e.g. so as not to highlight to a 'suspect' requesting access that an investigation into their activities or misconduct is underway and providing access to their personal information would prejudice the investigations). It is prudent to retain a copy of those written reasons in order to avoid any confusion in the event of a dispute.

Where access is denied, the charity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the charity and the individual. This is intended to ensure that entities work with individuals to try to satisfy their request. It may be that the use of a mutually agreed intermediary may permit sufficient access.

13.1.16 *Time periods*

A charity must respond to access requests within a reasonable period after the request is made. It is intended that a 'reasonable period' relating to more complicated requests will not usually exceed 30 days.

14. CORRECTION (APP 13)

Requirements

14.1.1 If a charity holds personal information and either:

(a) the charity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(b) the individual requests the entity to correct the information,

the charity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading (APP 13.1).

14.1.2 If the charity corrects personal information about an individual that the charity previously disclosed to another entity, and the individual requests that other entity be notified of the correction, then the charity must take such steps (if any) as are reasonable in the circumstances to give that notification, unless it is impracticable or unlawful to do so (APP 13.2).

14.1.3 Where correction is denied, the charity must give written notice of the reasons for refusal (except where unreasonable to set that out) and the mechanisms available to complain about the refusal (APP 13.3).

14.1.4 If the charity refuses to correct the information and the individual requests the charity to associate with the information a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading, then the charity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information (APP 13.4).

14.1.5 If a request is made under APP 13.1 or APP 13.4, the charity must respond to the request within a reasonable period after the request is made, and must not charge the individual for making the request, for correcting the information or for associating the statement with the information (APP 13.5).

14.1.6 *General obligation*

The principle is not intended to create a broad obligation on entities to maintain the correctness of personal information it holds at all times. The principle will interact with APP 10 (quality of personal information) so that when the quality of personal information is assessed at the time of use or disclosure, the charity may need to correct the information prior to that use or disclosure where it is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading.

Charities should establish a standard procedure for dealing with correction requests and complaints about its compliance with the correction provisions. Charities should also establish a standard procedure for, at the time of use or disclosure of information, assessing the quality of that information and whether it may need to correct that information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

14.1.7 *'Reasonable steps' to correct and notify of correction*

If personal information is held for a range of purposes, and it is considered incorrect with regard to one of those purposes, the obligation to take reasonable steps to correct the information should apply.

Where a charity corrects the personal information of an individual, it will be required to take reasonable steps to notify any other entity to which it had previously disclosed the

information, if that notification is requested by the individual. The compliance burden will be reduced by the proviso that notification is not required if it would be impracticable or unlawful.

14.1.8 *Statement relating to information*

If a charity refuses to correct personal information in response to an individual's request, APP 13.4 provides a mechanism for individuals to request that a statement that the information is inaccurate, out of date, incomplete, irrelevant or misleading be associated with the information. The charity must take reasonable steps to associate with the personal information a statement so that it is apparent to users of the personal information that the individual has sought correction of that information. This will ensure that individuals retain control of how their personal information is handled. The statement should address matters relevant to the information being inaccurate, out of date, incomplete, irrelevant or misleading, and should not be unreasonably lengthy. The appropriate content and length of any statement will depend on the circumstances of the matter.

14.1.9 *Time periods*

A charity must respond to correction requests within a reasonable period after the request is made. It is intended that a 'reasonable period' relating to more complicated requests will not usually exceed 30 days.

Part 3: Specific issues

15. SPAM AND TELEMARKETING

The Privacy Act, *Spam Act 2003* (Cth) ('**Spam Act**') and the *Do Not Call Register Act 2006* (Cth) ('**DNCR Act**') have different approaches for charities.

There is no exemption for charities in the Privacy Act.

15.1 Spam Act

15.1.1 The Spam Act:

(a) prohibits the sending of unsolicited commercial electronic messages (email, SMS or similar electronic media which, amongst other things, offer to supply or promote goods or services or a supplier) without the consent of the electronic account holder;

(b) requires the inclusion of a functional unsubscribe facility in any commercial electronic messages; and

(c) obliges persons or organisations sending commercial electronic messages to properly identify themselves.

15.1.2 There is a partial exemption from the Spam Act for some charities through provisions relating to 'designated commercial electronic messages'. A message is a designated commercial electronic message if it is a message that:

(a) has been authorised by a registered charity (amongst others);

(b) relates to goods or services; and

(c) the registered charity is the supplier of those goods or services.

15.1.3 A 'registered charity' means an entity that is registered under the *Australian Charities and Not-for-profits Commission Act 2012* (Cth) as the type of entity mentioned in column 1 of item 1 of the table in subsection 25.5(5) of that Act.

15.1.4 If an electronic message is a 'designated commercial electronic message' the general prohibition on sending unsolicited commercial electronic messages will not apply. The person authorising the message will also be exempt from the requirement to provide a functional unsubscribe facility (subject to the comments in paragraph 15.1.5 below). However, the exemption is only partial and, in particular, the charity sending or authorising the designated commercial electronic message must properly identify itself in the message.

15.1.5 If the commercial electronic message is direct marketing material, APP 7 will apply to the extent that the Spam Act does not apply (i.e. to the extent that the charity is exempt from the Spam Act). As such, although a registered charity may not have to provide a functional unsubscribe facility in a commercial electronic message under the Spam Act, under APP 7:

(a) the charity will be required to provide a simple means by which the individual may easily request not to receive direct marketing communications from the charity; and,

depending on whether the information was collected from the individual and whether the individual would reasonably expect their information to be used for direct marketing, the charity may be required to:

(b) obtain the individual's consent to the use of their information for direct marketing (unless it is impracticable to obtain consent); and

(c) include in the message a prominent statement that the individual may request not to receive direct marketing material from the charity.

15.1.6 Best practice is for charities to include an unsubscribe mechanism in all commercial

electronic messages or other direct marketing material.

15.2 DNCR Act

15.2.1 The DNCR Act allows people to register themselves on the Do Not Call Register. The Act prohibits persons and organisations from making telemarketing calls to persons who are on the register.

15.2.2 However, the prohibition does not extend to 'designated telemarketing calls'. The definition of designated telemarketing calls includes calls authorised by a registered charity where, if the call relates to goods or services, the charity is the supplier of the goods or services.

15.2.3 'Registered charity' has the same meaning as in the Spam Act (see paragraph 15.1.3 above).

15.2.4 Although registered charities are exempt from the DNCR Act, if the telemarketing call is direct marketing, they will need to comply with the requirements of APP 7. The requirements of APP 7 are set out in Section 8.

16. EMPLOYEE RECORDS

16.1.1 An act done, or practice engaged in, by an APP Entity that is or was an employer of an individual is exempt from the scope of the Privacy Act if the act or practice is directly related to:

(a) a current or former employment relationship between the employer and the individual; and

(b) an employee record held by the employer relating to the individual.

16.1.2 An 'employee record' is defined broadly to be a record of personal information relating to the employment of an employee. Examples of this type of information include the terms and conditions of employment, personal contact details, performance and conduct, disciplining, salary, termination and trade union membership.

16.1.3 Importantly for charities, the employee records exemption does not extend to volunteers. It also does not extend to prospective employees, contractors or consultants. Therefore, under the access provisions in APP 12 (see Section 13), volunteers, prospective employees, contractors and consultants may seek access to records of personal information which the charity holds about them. The charity should be mindful of this when collecting personal information (e.g. references, making notes and reports).

16.1.4 In New South Wales the health records of an employee will not be considered to be 'personal information' under the *Health Records And Information Privacy Act 2002* (NSW) and will not be covered by that legislation. In the Australian Capital Territory and Victoria, there is no such exemption in relation to the collection, use and disclosure of an employee's health records in the applicable State/Territory health records laws.

16.1.5 To be exempt, the act of the employer in relation to the employee record must be directly related to the current or former employment relationship. For example, if an employee of a charity seeks assistance in a personal matter from one of the charity's publicly available services, the use of this information is not exempt from the Privacy Act as it is not directly related to the employment relationship (see *C v Charity* [2011] PrivCmrA 3). Charities should have systems in place to avoid confusion between an individual acting as a client of one of its services, and as an employee.

17. USE OF PATIENT DATA

17.1.1 The use of patient data by hospitals or other entities supporting a client to solicit donations is a practice which needs careful review.

17.1.2 A patient's name and address is sensitive (health) information as, in the hands of the hospital, it indicates that the identified person has been receiving medical treatment. On the other hand, the details of the guardian or the next of kin of the patient (Associate) will not constitute health information as it only indicates the person has a connection with a patient, not that they have a medical condition.

17.1.3 Sensitive information of an individual may only be used and disclosed for the primary purposes for which it was collected or a directly related secondary purpose of which the individual is aware. It is unlikely that soliciting donations would be regarded as a directly related purpose and, generally, consent should be obtained.

17.1.4 However, it would be permissible to use the particulars of an Associate of the patient PROVIDED that the Associate was made aware that their personal information may be used for that purpose. Providing an appropriate notice of this use to Associates may prove difficult.

17.1.5 The use of patient information or their Associates to solicit donations is also likely to constitute direct marketing. Again, the patient's personal information cannot be used for this purpose without consent because it is sensitive information.

17.1.6 The situation is more complicated with the Associate of the patient. If the Associate themselves provided their personal information and the Associate would reasonably expect their personal information to be used to solicit donations, consent is not necessary but the hospital must provide a simple means for the individual to opt-out of receiving requests for donations. If the Associate's personal information was provided by a third party, such as the patient, and if it is 'impracticable' to gain the Associate's consent then there must be a prominent statement in each communication to the Associate seeking donations which advises that the Associate can opt-out of receiving further communications.

17.1.7 The above difficulties indicate that if a hospital or other institution wishes to use the personal information of a patient or an Associate of the patient, they should seek the informed consent to do so.

17.1.8 Consents can be express or implied. However, the Information Commissioner's Guidelines state that consent cannot be implied by just informing someone of the use to which their information is to be put. Rather, consent may only be provided by an individual taking a positive action to affirm or deny their consent.

17.1.9 If organisations wish to use opt-out consents the fact that it may be used to solicit donations must be clearly stated and a tick box provided which enables them to opt-out. The use of opt-ins is recommended so the individual is asked to tick a box to indicate they wish to receive communications.

17.1.10 Any consent for this use should not be bundled with other consents.

18. THIRD PARTY-SUPPLIED LISTS

18.1.1 Where a charity receives the name of a potential donor from a third party (such as a list provider or a data pooling arrangement) unless consent has been obtained, it must provide a simple means for the individual to easily request not to receive direct marketing communications (in the OAIC's Privacy business resource 19: Direct Marketing, the OAIC states that fundraising is considered a form of direct marketing). It must also include a prominent statement that the individual may make such a request or otherwise draw this to the individual's attention (APP 7.3). This could be achieved by providing a functional unsubscribe in electronic communications or a tick box to opt-out on a hard-copy form.

18.1.2 Charities must, on request, also be able to provide any individual whose personal information has been obtained via third-party lists with the source from which the charity obtained the individual's personal information (APP7.6). Any requests by individuals for this information must be notified to the individual within a reasonable period after the request was made (APP 7.7). Therefore, it is important that charities maintain accurate, current and accessible records of any third-party lists it obtains.

18.1.3 Further information about direct marketing can be found in Section 8.

19. USE OF SOCIAL MEDIA

19.1.1 Charities are increasingly using social media channels (e.g. Facebook, LinkedIn) to obtain information, including contact details, about actual or potential donors and track their profiles.

19.1.2 Not all personal information that is posted on social media sites that is viewed by charities will be 'collected' by a charity. For personal information to be considered to have been 'collected', it has to be held by the charity, i.e. the charity makes a record of personal information that is posted on social media. Where charities collect personal information via social media, they are still required to comply with the APPs when handling that information.

19.1.3 In particular, charities should consider:

(a) the requirements for collecting personal information and be careful not to collect personal information unless it is reasonably necessary for the charity's activities or functions, and especially consider the need to collect sensitive information (section 6);

(b) whether their use or disclosure of personal information collected from social media sites meets the requirements of APP 6 (refer to Section 7); and

(c) the requirements for sending direct marketing (including requests for donations), as referred to in Sections 8 and 15.

19.1.4 Charities may also have their own social media policies, which govern the use of social media by a charity's personnel.

Part 4: Complaints handling and data breaches

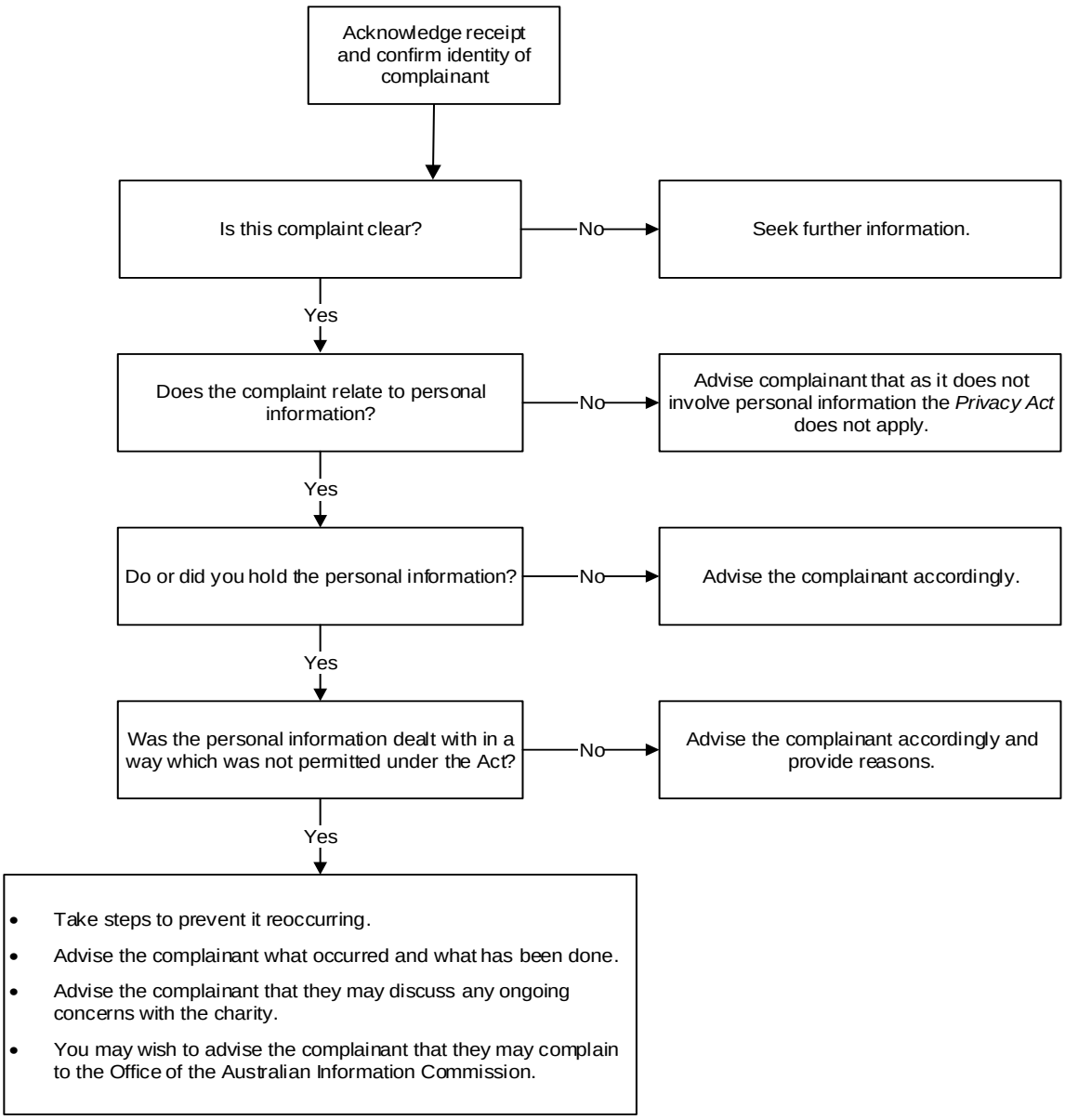
20. COMPLAINTS HANDLING PROCEDURE

20.1.1 APP 1.2(b) requires a charity to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the charity's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs.

20.1.2 Complaints should be directed in the first instance to the charity. The Information Commissioner may decide not to investigate a matter if the individual has not first brought a complaint to the charity concerned, unless the Information Commissioner is of the view that this would be inappropriate.

20.1.3 The diagram below illustrates the steps that a charity could take on receipt of a complaint.

Procedure on Receiving Complaint



20.1.4 Charities are also required to:

(a) advise individuals in their collection statement that their Privacy Policy contains information about how the individuals may complain about a breach of the APPs and how the charity will deal with the complaint; and

(b) advise individuals in their Privacy Policy of how the individuals may complain about a breach of the APPs and how the charity will deal with that complaint.

20.1.5 If the complaint is unable to be resolved at the charity level, the Information Commissioner may investigate the complaint.

20.1.6 The enforcement options available to the Information Commissioner are outlined in Section 1.3.

21. RESPONDING TO DATA BREACHES

21.1 Introduction

21.1.1 A data breach concerns the security of personal information and involves the actual unauthorised access or disclosure of personal information, or the loss of personal information where the loss is likely to result in unauthorised access or disclosure (**Data Breach**).

21.1.2 Data Breaches are not limited to the malicious acts of third parties, such as theft or 'hacking', but may also arise from human error, a systems failure, or a failure to follow information handling or data security policies resulting in accidental loss, access or disclosure. Data Breaches are different from an interference with privacy that involves a breach of another APP such as a use or disclosure of personal information which is not permitted under APP6 (see ' Section 7 – Use or disclosure of personal information). The following are examples of when a Data Breach may occur:

(a) loss of smartphone or other charity device or equipment containing personal information;

(a) cyber-attacks on a charity's system, resulting in unknown third parties accessing or stealing personal information;

(b) accidental transmission of personal information such as donor's details to unintended recipients via e-mail;

(c) loss or theft of hard-copy documents; and

(d) misuse of personal information of by a charity's personnel.

21.1.3 All charities with personal information security obligations under the Privacy Act are required to report certain types of data breaches under the notifiable data breaches scheme (**NDB Scheme**) set out in the Act. The NDB Scheme sets out obligations to notify affected individuals and the Information Commissioner about data breaches which fall within the definition of an 'eligible data breach' (**EDB**).

21.1.4 A Data Breach is an EDB if it is likely to result in serious harm to an individual or individuals whose information is involved in the Data Breach. Not all Data Breaches will be EDBs. For example, if a charity acts quickly to remediate a Data Breach, and as a result of this action the Data Breach is not likely to result in serious harm, there is no obligation to notify any individuals or the Information Commissioner. There are also limited exceptions to notifying affected individuals and the Information Commissioner of an EDB in certain circumstances.

21.1.5 This section provides guidance for charities regarding:

(a) containing a Data Breach;

(b) assessing whether a Data Breach is an EDB and taking remedial action to reduce the likelihood of harm to individuals affected by the Data Breach;

(c) notifying the Information Commissioner of an EDB and notifying individuals affected by an EDB, and potential exceptions to notification; and

(d) reviewing the Data Breach/EDB.

21.2 Containing the Data Breach

21.2.1 Once a charity suspects a Data Breach may have occurred, immediate steps should be taken to identify the Data Breach and if a Data Breach has occurred, to contain and limit it. This may involve stopping the unauthorised disclosure, shutting down the system that was

breached, retrieving personal information, or changing computer access privileges or addressing security weaknesses.

21.3 Assessing whether the Data Breach is an EDB

21.3.1 Charities also need to determine whether the Data Breach is an EDB. This involves assessing whether:

(a) there has been unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information in circumstances where the loss is likely to result in unauthorised access or disclosure; and

(b) if so, the Data Breach is likely to result in serious harm to any of the individuals whose personal information was involved; and

(c) remedial action is possible.

21.3.2 Is serious harm likely?

(a) Determining whether serious harm is likely is a threshold test and involves considering whether a reasonable person in the charity's position would conclude that the Data Breach would be likely (more probable than not) to result in serious harm to any of the individuals to whom the information relates.

(b) This reasonable person test is aimed at ensuring only EDBs are reported to the Information Commissioner – not every Data Breach. EDBs will be Data Breaches that:

(i) a reasonable person in the charity's position (rather than the individual to whom the information relates or any other person) would conclude;

(ii) based on all of the information either immediately available to them or available following reasonable inquiries or an assessment of the data breach; and

(iii) that the unauthorised access to or disclosure of the particular personal information or the particular individual, is likely to result in serious harm to them.

(c) This test is designed to support the objective of the Privacy Act to promote the protection of the privacy of individuals while balancing the interests of entities carrying out their legitimate functions or activities. It also helps avoid unnecessary administrative burdens (both on entities such as charities, and on the OAIC receiving notification), and 'notification fatigue' on the part of individuals.

21.3.3 What is serious harm?

(a) Serious harm is not defined in the Privacy Act; however, in the context of a Data Breach, the OAIC Resources note that serious harm may include serious physical, psychological, emotional, financial or reputational harm. The Privacy Act also sets out a non-exhaustive list of 'relevant matters' that may assist charities in assessing the likelihood of serious harm. These include:

(i) the kind or kinds of personal information involved;

(ii) the sensitivity of that information;

(iii) whether the information is protected by one or more security measures and the likelihood any such security measures would be overcome, including the use of an encryption key to circumvent the encryption technology or methodology;

(iv) the person, or the kinds of persons, who have obtained, or who could obtain, the information;

(v) the likelihood that the person who has obtained the information, or has or could obtain, the information or knowledge required to circumvent the security technology or methodology;

(vi) the nature of the harm; and

(vii) any other relevant matters.

21.3.4 Only those individuals whose information has been affected by a Data Breach and who are likely to suffer serious harm need to be notified. If the charity assesses that the risk to some affected individuals does not reach this threshold, then they do not need to be notified.

21.3.5 Can serious harm be prevented with remedial action?

(a) As part of assessing the likelihood of serious harm, charities should take steps to consider whether remedial action to reduce any potential harm to individuals is possible (to prevent serious harm). The NDB Scheme provides that if entities take remedial action to prevent the serious harm resulting from the Data Breach, then it will not be an EDB that must be notified. The charity will need to assess whether the effect of the action it takes would mean that the Data Breach would not be likely to result in serious harm to any of the individuals to whom the affected information relates, in relation to any remedial action. This may include action taken in relation to:

(i) the access or disclosure that has occurred *before* the access or disclosure results in serious harm to any of the individuals to whom the information relates; or

(ii) the loss information *before* there is unauthorised access to or disclosure of the information so that there is no unauthorised access or unauthorised disclosure; or

(iii) the loss of information *after* there is an unauthorised access to or disclosure but *before* the access or disclosure results in serious harm to any of the individuals to whom the information relates.

21.3.6 Timing of the assessment

(a) If a charity suspects an EDB may have occurred, they should take reasonable steps to conduct this assessment expeditiously, and where possible, within 30 days after the suspicion arises that a Data Breach has occurred.

21.3.7 What if multiple organisations are involved in the EDB or suspected EDB?

(a) If a charity or other organisation (e.g. a cloud service provider or other third party supplier) are together involved in a Data Breach affecting personal information of individuals the charity handles, and either the charity or other organisation has made an assessment about a suspected Data Breach to determine whether there has been an EDB, the charity or other organisation involved in the Data Breach is not required to undertake the same assessment and may rely on the assessment already made. However, in some cases, charities may also want to undertake their own assessment or may have information that would help determine whether serious harm is likely to any individual. Charities should ensure their contracts with third-party service providers make the responsible duties of the provider clear.

21.4 Notifying affected individuals and the Information Commissioner

21.4.1 Once a charity is aware that there are reasonable grounds to believe there has been an EDB, the charity must, as soon as practicable:

(a) make a decision about which individuals to notify;

(b) prepare a statement for the Information Commissioner in accordance with the OAIC *Notifiable Data Breach statement – Form* – this can be emailed or lodged online via the OAIC website: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB; and

(c) notify affected individuals of this statement as soon as practicable after notifying the Information Commissioner.

21.4.2 The charity will still need to be continuing to take what steps it can to contain the Data Breach and minimise the likely harm as well as deciding what steps it would recommend the individuals can take to protect themselves as it will need to explain this in the statement it must give to the Information Commissioner and individuals, as explained below.

21.4.3 The NDB Scheme provides three options for notifying affected individuals of the statement provided to the Information Commissioner:

(a) Option 1: notify all individuals whose personal information was part of the EDB;

(b) Option 2: notify only those individuals at risk of serious harm from the EDB; or

(c) Option 3: if neither option 1 or 2 are practicable, the charity must publish a copy of the statement provided to the Information Commissioner on its website if it has one and take reasonable steps to publicise the contents of the statement.

21.4.4 A charity can use any reasonable method to notify individuals via option 1 or 2 (e.g. telephone call, SMS, physical mail, social media post, or in-person conversation), or their usual method of communicating with that individual.

21.4.5 Charities can tailor the notification to individuals, as long as it includes the content of the statement charities must provide to the Information Commissioner. The NDB Scheme requires the statement and the notification to individuals to include:

(a) the identity and contact details of the charity;

(b) a description of the EDB that the charity has reasonable grounds to believe has happened;

(c) the kind, or kinds, or information concerned;

(d) recommendations about the steps that individuals should take in response to the EDB.

21.4.6 There are limited relevant exceptions to charities' obligations to notify the Information Commissioner and/or individuals. These are

(a) if the EDB affects the security of personal information held by multiple organisations, only one organisation needs to prepare the statement and give notification of the EDB, for all affected organisations to comply with the notification requirements under the NDB Scheme; and

(b) where the Information Commissioner makes a declaration that an entity is not required to comply with the notification requirements under the NDB Scheme or can delay giving that notice. This declaration can be made as a result of a submission by the charity about reasons why notification to the Information Commissioner or some or all of the individuals should not be made or delayed, e.g. there is a police investigation which may be compromised or the individual would be at risk if notified.

21.4.7 Whilst not mandatory, in some circumstances it may be appropriate to also notify third parties such as:

(a) Police or law enforcement – if theft of other crime is suspected – it can be an offence in some States not to notify an indictable offence to the police;

(b) Credit card companies or financial institutions – e.g. if the charity or a service providers have obligations under other regulatory schemes such as credit card payment processors who are subject to the Payment Card Industry Security Standards or their assistance is necessary for contacting individuals or mitigating harm;

(c) Other internal or external parties not already notified – if they may be impacted by the EDB (e.g. professional bodies, or the ATO if Tax File Numbers are affected); and

(d) the Australian Cyber Security agencies such as the ACS Centre, including National Computer Emergency Response Team (CERT) or the Australian Cyber Crime Online Reporting Network (ACORN), if the charity has been a victim of cyber-crime. They can offer further advice and support in relation to cyber security incidents and a report can be lodged and followed up by the appropriate agency.

21.4.8 Charities who offer goods and services to or target individuals based in the European Union (EU), or monitor their behaviour there and collect and hold their data, still need to consider if European General Data Protection Regulation (**GDPR**) applies to them and, if so, how they will meet the data breach notifications obligations in the GDPR which are more onerous.

21.5 Reviewing the Data Breach/EDB

21.5.1 Whether the incident that occurs is a Data Breach or an EDB that requires notification under the NDB Scheme, conducting a follow-up review of the Data Breach once the above steps have been taken is very important so that charities take action to prevent future breaches and ensure ongoing compliance with their data security obligations and overarching obligation to manage the personal information they hold in a compliant manner. This includes:

(a) investigating and understanding the cause(s) of the Data Breach or EDB;

(b) developing a prevention plan and conducting audits to ensure the plan is implemented;

(c) considering changes to policies and procedures; and

(d) further staff training.

21.6 Consequences

21.6.1 The NDB Scheme is subject to the existing regulatory and enforcement framework overseen by the Information Commissioner and OAIC as set out in the Privacy Act. This means that the consequences of a charity breaching a requirement of the NDB Scheme, include:

(a) an investigation by the Information Commissioner into the causes of the Data Breach/EDB and the charity's response;

(b) a determination by the Information Commissioner that the charity take specified steps to remedy non-compliance, perform any reasonable act to redress any loss suffered, pay monetary compensation;

(c) a request that the charity provide an enforceable undertaking that it will take, or refrain from taking, specified action in the case of serious or repeated noncompliance; or

(d) an application by the Information Commissioner to court to impose a civil pecuniary penalty of up to $2.1 million per breach.

21.7 Voluntary notification

21.7.1 Even when the Data Breach is not an EDB under the NDB Scheme, there may be instances where a charity considers it necessary to voluntarily notify one or some affected individuals of a Data Breach, in accordance with its obligations under APP 11 to take reasonable steps to keep the personal information it holds secure (see Section 12) as well as for managing the reputational impact to the charity. The Information Commissioner's preference is that organisations should only report 'eligible breaches' under the NDB Scheme to the OAIC. That is, charities should not report breaches to the OAIC out of an abundance of caution if a breach is not assessed to be eligible.

21.8 Data Breach Response Plan

21.8.1 To help charities meet their NDB Scheme obligations and effectively respond to and manage Data Breaches, they should prepare a documented Data Breach Response Plan based on the above guidance. This should include the breach response team, identify how breaches should be escalated, and tested and kept under regular review.

Annexure 1 – Summary of obligations under the APPs

1. Manage personal information in an open and transparent way.
2. Take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the charity's functions or activities that:
   (a) will ensure compliance with the APPs; and
   (b) will enable the charity to deal with inquiries or complaints about compliance with the APPs.
3. Have a clearly expressed and up-to-date published Privacy Policy about the charity's management of personal information.
4. If it is lawful or practicable, give individuals the option of interacting anonymously with the charity or using a pseudonym.
5. Only collect personal information that is reasonably necessary for the charity's functions or activities.
6. Obtain consent to collect sensitive information unless specified exemptions apply.
7. Use fair and lawful means to collect personal information.
8. Collect personal information directly from an individual if it is reasonable and practicable to do so.
9. If the charity receives unsolicited personal information, determine whether it could have collected the information under APP 3 as if it had solicited the information. If so, APPs 5-13 will apply. If not, the information must be destroyed or de-identified.
10. Before or at the time the charity collects personal information or as soon as practicable afterwards, take such steps (if any) as are reasonable in the circumstances to make an individual aware of:
    (a) why the charity is collecting information about them;
    (b) who else the charity might give it to; and
    (c) other specified matters.
11. Take such steps (if any) as are reasonable in the circumstances to ensure the individual is aware of this information even if the charity has collected it from someone else.
12. Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in APP 6.2 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances).
13. If the information is sensitive, the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the primary purpose of collection.
14. Do not use personal information for direct marketing, unless one of the exceptions in APP 7 applies (for example, the charity has obtained consent or where the individual has a reasonable expectation of their information being used or disclosed for that purpose and the charity has provided a simple means for the individual to unsubscribe from such communications). APP 7 does not apply if the Spam or DNCR Acts apply.
15. Before the charity discloses personal information to an overseas recipient it must take such steps as are reasonable in the circumstances to ensure that the recipient does not

breach the APPs, and it will remain accountable for the handling of the information by the overseas recipient, unless an exception applies.

16. Government-related identifiers must not be adopted, used or disclosed unless one of the exceptions applies (e.g. the use or disclosure is reasonably necessary to verify the identity of the individual for the purposes of the charity's functions or activities).

17. Take such steps (if any) as are reasonable in the circumstances to ensure the personal information the charity collects, uses or discloses is accurate, complete and up to date. This may require the charity to correct the information if requested or on its own motion and possibly advise organisations to whom it has disclosed the information of the correction.

18. Take such steps as are reasonable in the circumstances to protect the personal information the charity holds from misuse, interference and loss and from unauthorised access, modification or disclosure.

19. Take such steps as are reasonable in the circumstances to destroy or permanently de-identify personal information no longer needed for any purpose for which the charity may use or disclose the information.

20. If requested, the charity must give access to the personal information it holds about an individual unless particular circumstances apply that allow it to limit the extent to which it gives access.

21. If a charity refuses an access or correction request, it must give written reasons for the refusal and explain how the individual can complain.

Note: This is a summary only and NOT a full statement of obligations.

Annexure 2 – Privacy planning template

Personal Information (PI) collected	Needed for a function or activity of charity?	From whom is the PI collected?	Where is the PI recorded?	Who can access each class of information?	How long kept?	Level of security risk[1]	Disclosed outside charity?	Held or processed by a contracted vendor?
	Y/N		P=Paper file E=Electronic database			H=High M=Medium L=Low	Y/N	Y/N
Name								
Address								
Phone number(s)								
Date of birth (& age)								
Other (list)								

[1] Considering the nature of the information, type of storage, access and possible disclosure

Annexure 3 – Template Privacy Policy

The following Privacy Policy is a template only and must be adapted to reflect each charity's particular acts and practices.

Wording in square brackets indicates wording that should be replaced with the relevant information (such as the charity's name) or that is unlikely to apply to all charities and should be retained or deleted as applicable.

Privacy Policy

This Privacy Policy outlines how [charity name] collects, handles and safeguards your personal information. It also outlines how you can seek to access and correct your personal information and make a privacy complaint.

Information we collect and how we use and disclose it

[***Note: Insert the categories of individuals as relevant to the charity. If a charity collects information from other individuals, new categories should be added. Examples of other categories could include healthcare professionals, participants at events and members of the charity.***]

Individuals who we assist **[Note: Where the policy appears on the charity's website, if possible, these titles (of categories of individuals) should be a drop-down menu]**

1. What information do we collect about you and how?

The kinds of personal information we collect about you depends on who you are and include your name, date of birth and contact details. [We may also collect your sensitive information (which includes health information), such as information about your disability.]

We collect most of your personal information directly from you, including via telephone, via email, when you attend one of our events, and when you otherwise interact with us. We may also collect your personal information from third parties such as other charities, social media and [others].

2. Why do we need your personal information?

We collect, hold, use and disclose your personal information:

(a) to provide our goods and services to you and enable you to participate in our programs;

(b) to enable us to communicate with you about the goods or services we are providing you or the program you are participating in;

(c) to inform you about our [and third parties'] goods, services and/or programs which we think you may be interested in;

(d) to improve our goods, services and programs;

(e) [to apply for subsidies and grants]; and

(f) to comply with our legal obligations.

3. To whom do we disclose personal information?

We may disclose your personal information to third parties who assist us in supplying our goods, services and programs or who perform functions on our behalf, to other third parties where required by law and to anyone else to whom you authorise us to disclose it.

[We may also disclose your personal information to relevant Government agencies to apply for subsidies and grants.]

[We do not currently disclose your personal information to overseas recipients.][These third-party recipients may be located overseas, including in [insert countries].]

[From time to time, we may compile statistical data from the personal information we have collected. In these instances, the data will be aggregated and de-identified before it is disclosed to third parties.]

[We may disclose your personal information to service providers who help us with our functions and activities including [insert usual providers, e.g. marketing services]]

Donors

1. What information do we collect about you and how?

The kinds of personal information we collect about you include your name, contact details and credit card or other payment details.

We collect your personal information directly from you when you provide your information to us in person, in writing, via email, via the telephone or on our website when donating funds to us. We may also receive your personal information from other charities [or third parties that have provided us with lists to identify prospective donors].

2. Why do we need your personal information?

We collect, hold, use and disclose your personal information to enable us to process your donation, communicate with you about your donation and inform you about our [and third parties'] goods, services and/or programs which we think you may be interested in.

3. To whom do we disclose your personal information?

Unless you ask us not to, we may publicly acknowledge you as a donor.

We may also disclose your personal information to third parties who assist in processing our donations such as payment processors, [other charities (including to enable them to send you information about their goods, services and programs)], other third parties where required by law and to anyone else to whom you authorise us to disclose it.

[We do not currently disclose your personal information to overseas recipients.][These third-party recipients may be located overseas, including in [insert countries].]

Volunteers / Contractors

1. What information do we collect about you and how?

The kinds of personal information we collect about you include your name, date of birth, contact details, gender, work history, any other information you include in your application and, in respect of contractors, payment details.

[We may also collect sensitive information about you, relating to your ability to provide services to us and your criminal record history.]

We collect this personal information directly from you when you provide your information to us in writing, via email, via the telephone or on our website when applying, enquiring, or registering for opportunities with us. We also collect information from your nominated referees, and [through criminal history and working with children checks.]

2. Why do we need your personal information?

We may collect, hold, use and disclose your personal information to assess your application, allow you to provide services to us (including communicating with you about those services), provide training to you, communicate with you about opportunities with us, improve our services, [inform you about our [and third parties'] goods, services and/or programs which we think you may be interested in] and comply with our legal obligations.

3. To whom do we disclose your personal information?

We may disclose your personal information to [individuals participating in our programs], third parties who assist us in supplying our goods, services and programs or who perform functions on our behalf, [other charities (including to enable them to send you information about their goods, services and programs)], other third parties where required by law [(,including Government agencies to conduct criminal history and working with children checks)] and to anyone else to whom you authorise us to disclose it.

[We do not currently disclose your personal information to overseas recipients.][These third-party recipients may be located overseas, including in [insert countries].]

Prospective employees

1. What information do we collect about you and how?

The kinds of personal information we collect about you include your name, date of birth, contact details, gender, information about your employment history, tax file number, bank account details, referee information and information you provide in a CV or interview.

[We may also collect sensitive information about you, relating to your ability to work with us and your criminal record history.]

We collect this personal information directly from you when you provide your information to us in writing, via email, via the telephone or on our website when applying, enquiring, or registering for employment opportunities with us. We also collect information from your nominated referees, and [through criminal history and working with children checks.]

2. Why do we need your personal information?

We collect, hold, use and disclose your personal information to assess your suitability for employment with us and to comply with our legal obligations.

3. To whom do we disclose your personal information?

We may disclose your personal information to [third parties who assist us in our recruitment processes], to third parties where required by law [(,including Government agencies to conduct criminal history and working with children checks)] and to anyone else to whom you authorise us to disclose it.

[We do not currently disclose your personal information to overseas recipients.][These third-party recipients may be located overseas, including in [insert countries].]

Storage and security

We hold personal information in electronic and hard-copy files. [We may store your information with a third-party storage provider.]

[We may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside Australia.]

We takes reasonable steps to protect personal information from misuse, interference and loss and from unauthorised access, modification and disclosure. These steps include [insert the steps taken by the charity to secure personal information, including physical security, logical security and access and use restrictions.]

We take reasonable steps to ensure that when the information is no longer needed, it is destroyed or permanently rendered anonymous.

How to access or correct your personal information

You may at any time request access to, or correction of, the personal information we hold about you by contacting the Privacy Officer using the contact details below. We will seek to respond to your request as soon as practicable.

You may be charged an administration fee when we provide you with access to the requested information. However, you will not be charged for making an access or correction request, or for the correction of your personal information.

Complaints

If you wish to make a complaint about a breach of any privacy laws by [charity name], please contact our Privacy Officer using the details below.

We may request that you make your complaint in writing. We will investigate any complaint and will notify you of our decision in relation to your complaint as soon as is practicable after it has been made (usually within 30 days).

You may also contact the Office of the Australian Information Commissioner (visit oaic.gov.au for further information).

Contact our Privacy Officer

If you have any questions relating to this Privacy Policy please contact our Privacy Officer:

[insert postal address]
[insert email address]

[insert phone number]

Updates to this Privacy Policy

This Privacy Policy may be updated from time to time. The current version will be published on [this website][or insert website address].

Version date: [insert date]

Annexure 4 – Collection notices

The following collection notices are templates only and must be adapted to reflect each charity's particular acts and practices. A charity may need to develop additional collection notices depending on the individuals from whom it collects personal information.

Wording in square brackets indicates wording that should be replaced with the relevant information (such as the charity's name) or that it is unlikely to apply to all charities and should be retained or deleted as applicable.

It is assumed that:
(1) the contact details for the charity are provided to the particular individual elsewhere; and
(2) there are no significant, non-obvious consequences of the individual not providing their personal information.

If not, these details should be included in the notices.

1. Donor collection notice

In making a donation to [insert charity], you will be providing us with your personal information. We may also receive your personal information from other charities [or third parties that have provided us with lists to identify prospective donors].

If you wish to remain anonymous or use a pseudonym when making a donation, you may do so by [insert mechanism].

We collect your personal information to enable us to process your donation, communicate with you about your donation and inform you about our [and third parties'] goods, services and/or programs which we think you may be interested in.

Unless you ask us not to, we may publicly acknowledge you as a donor. We may also disclose your personal information to third parties who assist in processing our donations, [other charities (including to enable them to send you information about their goods, services and programs)], other third parties where required by law and to anyone else to whom you authorise us to disclose it. [We do not currently disclose your personal information to overseas recipients.][These third party recipients may be located overseas, including in [insert countries].] [We may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside Australia.]

If you do not want us to send you information about the work of [insert charity] [, or to disclose your personal information to other charities so that they can send you marketing material,] [if form is online or being returned to company [please tick here [insert tick box]]/ [if form is not being returned to company] [please call us on [insert phone number]].

Our Privacy Policy located at [link to privacy policy] contains details of how you can seek to access or correct personal information we hold about you. It also contains information about how you can complain about a breach of the Australian Privacy Principles by us and how we will deal with your complaint.

2. Volunteer / contractor collection notice

[Charity name] collects your personal information when you apply to provide, and provide, services to us. We generally collect this personal information directly from you. However, we may also collect it from your nominated referees, and [through criminal history checks and working with children checks [as required by child protection laws].]

We collect your personal information to assess your application, allow you to provide services to us (including communicating with you about those services), provide training to you, communicate with you about opportunities with us, improve our services, [inform you about our [and third parties'] goods, services and/or programs which we think you may be interested in] and comply with our legal obligations.

Unless you advise us otherwise, we may keep your personal information in an electronic or hard-copy file for 12 months if your application is unsuccessful in case another opportunity becomes available.

We may disclose your personal information to [individuals participating in our programs], third parties who assist us in supplying our goods, services and programs or who perform functions on our behalf, [other charities (including to enable them to send you information about their goods, services and programs)], other third parties where required by law [(including Government agencies to conduct criminal history and working with children checks, Charities Common if a Board Member)] and to anyone else to whom you authorise us to disclose it. [We do not currently disclose your personal information to overseas recipients.][These third party recipients may be located overseas, including in [insert countries].] [We may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside Australia.]

If you do not want us to send you marketing material[, or to disclose your personal information to other charities so that they can send you marketing material,] please call us on [insert phone number].

If you provide us with the personal information of others (such as referees), we encourage you to inform them that you are disclosing that information to us and why, that they can access that information if they wish and that we do not usually disclose the information to third parties.

Our Privacy Policy located at [link to privacy policy] contains details of how you can seek to access or correct personal information we hold about you. It also contains information about how you can complain about a breach of the Australian Privacy Principles by us and how we will deal with your complaint.

3. Job applicant collection notice

[Charity name] collects your personal information when you apply for a position with us. We generally collect this personal information directly from you. However, we may also collect it from your nominated referees, and [through criminal history checks and working with children checks [(as required by child protection laws)].]

We collect this information in order to assess your application for employment and to comply with our legal obligations.

Unless you advise us otherwise, we may keep your personal information in an electronic or hard-copy file for up to 12 months if your application is unsuccessful in case another opportunity becomes available.

We may disclose your personal information to [third parties who assist us in our recruitment processes], to third parties where required by law [(including Government agencies to conduct criminal history and working with children checks)] and to anyone else to whom you authorise us to disclose it. [We do not currently disclose your personal information to overseas recipients.][These third party recipients may be located overseas, including in [insert countries].] [We may also store personal information in the 'cloud' which may mean that it resides on servers which are situated outside Australia.]

If you provide us with the personal information of others (such as referees), we encourage you to inform them that you are disclosing that information to us and why, that they can access that information if they wish, and that we do not usually disclose the information to third parties.

Our Privacy Policy located at [link to privacy policy] contains details of how you can seek to access or correct personal information we hold about you. It also contains information about how you can complain about a breach of the Australian Privacy Principles by us and how we will deal with your complaint.

Further information

Further information about specific issues which arise for charities can be obtained from MinterEllison's privacy team.

Sydney

John Fairbairn: +61 2 9921 4590
Anthony Lloyd: +61 2 9921 8648

Melbourne

Paul Kallenbach: +61 3 8608 2622
Veronica Scott: +61 3 8608 2126

Brisbane

Ian Lockhart: +61 7 3119 6210
Leah Mooney: +61 7 3119 6230

Canberra

Christina Graves: +61 2 6225 3349

Perth

Mike Hales: +61 8 6189 7825

Adelaide

Lisa Jarrett: +61 8 8233 5501