Prepared by Minter Ellison Lawyers

AUSTRALIAN CATHOLIC BISHOPS CONFERENCE

PRIVACY COMPLIANCE MANUAL

October 2014

The Australian Catholic Bishops Conference has published this Privacy Compliance Manual for its own use and the use of its agencies. Dioceses, parishes and other diocesan or parish agencies within the Catholic Church in Australia may also personalise, modify, use and copy this manual freely. This permission excludes supplying the original or modified documentation to any organisation that is not a diocese, parish or diocesan or parish agency within the Catholic Church in Australia.

Australian Catholic Bishops Conference
General Secretariat
GPO Box 368
CANBERRA ACT 2601

DISCLAIMER

This Manual is for guidance only. Individual Parishes, Dioceses or other organisations within the Church may wish to seek specific advice on how to comply with the Privacy Act.

TABLE OF CONTENTS

PART 1 – INTRODUCTION TO PRIVACY 5

1. Context 5
   1.1 Purpose of Manual 5
   1.2 Application of the Privacy Act 5
   1.3 Australian Privacy Principles 5

2. WHAT INFORMATION DOES THE ACT COVER? 6
   2.1 Regulation of 'personal information' 6
   2.2 What is 'sensitive information'? 6
   2.3 What is 'health information'? 6
   2.4 What is a 'record'? 6
   2.5 Consent 7
   2.6 Which acts and practices are exempt? 7

3. APP BREACHES AND COMPLAINTS 9
   3.1 Breach of the APPs 9
   3.2 Complaints 9
   3.3 Own motion investigations by the Privacy Commissioner 9
   3.4 Penalties 9

PART 2 – THE AUSTRALIAN PRIVACY PRINCIPLES 11

4. OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION (APP 1) 11
   4.1 Open and transparent management of personal information (APP 1) 11
   4.2 How to comply: 11
   4.3 Privacy Policy (APP 1.3-1.6) 12
   4.4 How to comply: 12
   4.5 Training staff 13
   4.6 Do's and Don'ts 13

5. ANONYMITY and PSEUDONYMITY (APP 2) 14
   5.1 Anonymity and Pseudonymity 14
   5.2 Comment 14
   5.3 How to comply: 14

6. COLLECTION (APP 3, 4, and 5) 15
   6.1 Collection 15
   6.2 Sensitive Information (APP 3.3 and 3.4) 15
   6.3 Comment 15
   6.4 How to comply: 16
   6.5 Lawful and fair collection (APP 3.5) 16
   6.6 Comment 16
   6.7 How to comply: 16
   6.8 Privacy collection statement - ensuring the individual is fully aware of collection (APP 5.1) 16
   6.9 Comment 17
   6.10 How to comply: 18

6.11 Collection through surveillance 18
6.12 Collection of information directly from the individual (APP 3.6) 19
6.13 Comment 19
6.14 How to comply: 19
6.15 Collection, use and disclosure with third parties and contractors (APP 3.6 and APP 6) 19
6.16 How to comply: 20
6.17 Collecting sensitive information with consent 20
6.18 Collecting sensitive information without consent 20
6.19 How to comply: 20
6.20 Collection Compliance Steps 22
6.21 Unsolicited Personal Information (APP 4) 22
6.22 Do's and Don'ts 23
6.23 Additional Do's and Don'ts for sensitive information 23

7. USE AND DISCLOSURE OF PERSONAL INFORMATION (APP 6) 24
7.1 Use and Disclosure 24
7.2 Primary and related purpose of collection 24
7.3 How to comply: 25
7.4 Use or disclosure required by law (APP 6.2(b)) 25
7.5 How to comply: 25
7.6 Use & Disclosure Compliance Steps 26
7.7 Do's and Don'ts 27

8. DIRECT MARKETING (APP 7) 28
8.1 Direct Marketing 28
8.2 Comment 29
8.3 How to comply: 30

9. CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION (APP 8) 31
9.1 Cross-border Disclosure 31
9.2 How to comply: 31
9.3 Using cloud storage providers 32
9.4 Do's and Don'ts: 33

10. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS (APP 9) 34
10.1 Identifiers 34
10.2 Comment 34
10.3 How to comply: 34
10.4 Do's and Don'ts: 34

11. DATA QUALITY (APP 10) 35
11.1 Data Quality 35
11.2 Comment 35
11.3 How to comply: 35
11.4 Sharing personal information 36
11.5 Do's and Don'ts 36

12. DATA SECURITY (APP 11) 37
12.1 Security of Personal Information 37
12.2 How to comply 37
12.3 Reasonable steps 38

12.4 How to comply: 38
12.5 Destruction and permanent de-identification (APP 11.2) 39
12.6 Comment 39
12.7 How to comply: 39
12.8 Do's and Don'ts 40

13. ACCESS (APP 12) 42
13.1 Access to Personal Information 42
13.2 Comment 43
13.3 How to comply: 43
13.4 Do's and Don'ts 45

14. CORRECTION 46
14.1 Correction of Personal Information (APP 13) 46
14.2 Comment 46
14.3 How to comply: 47
14.4 Do's and Don'ts 47

PART 3 SPECIAL ISSUES FOR THE CHURCH 48

15. CAPACITY TO CONSENT 48
15.1 Capacity 48
15.2 Consent and Young People 48

16. DUTY OF CARE AND OBLIGATIONS OF CONFIDENCE 50
16.1 Duty of Care, Obligations of Confidence and the APPs 50

17. PERSONAL INFORMATION AND THE CHURCH COMMUNITY 51
17.1 Passing Information in the Church Community 51
17.2 Religious Information 51
17.3 Fundraising 51
17.4 Passing personal information to other Church Bodies 51
17.5 Church Body Publications 51

18. HEALTH INFORMATION 53
18.1 Protection of Health Information 53
18.2 What is Health Information? 53
18.3 Collection of Health Information 53
18.4 Use or Disclosure of Health Information 54
18.5 Health Information and Employees 54
18.6 Additional Requirements in States and Territories 54
18.7 Inconsistencies between Federal and State laws 56

19. EMPLOYEE RECORDS 57
19.1 Employee Records 57
19.2 Recommendation 58

ANNEXURE 1 – TEMPLATE PRIVACY POLICY 59

ANNEXURE 2 – TEMPLATE COLLECTION STATEMENTS 64

PART 1 – INTRODUCTION TO PRIVACY

1. CONTEXT

1.1 Purpose of Manual

1.1.1 The purpose of the Manual is to assist parishes, dioceses and other organisations within the Church (**Church Bodies**) to comply with Australian privacy laws, including the *Privacy Act 1988* (Cth), (**Privacy Act**) and health records legislation.

1.1.2 Amendments to the Privacy Act by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), came into operation on 12 March 2014. The changes affect Church Bodies. The key changes are in the new Australian Privacy Principles (**APPs**) in the Privacy Act. The APPs replace the National Privacy Principles (**NPPs**) that were inserted into the Privacy Act in 2001. While the drafting of the APPs is different, overall the obligations on Church Bodies under the APPs are very similar to the obligations under the NPPs. However, Church Bodies need to observe some important changes.

1.2 Application of the Privacy Act

1.2.1 The Privacy Act through the APPs regulates different types of personal information collected and held by:

(a) Commonwealth and Australian Capital Territory government agencies; and
(b) private sector organisations with annual turnovers of over $3 million.

1.2.2 An 'organisation' includes:

(a) an individual;
(b) a body corporate;
(c) a partnership;
(d) any other unincorporated association; or
(e) a trust.

1.2.3 A Church Body is an 'organisation' for the purpose of the Privacy Act. While many Church Bodies do not separately have a turnover of over $3 million, they may effectively be related to an organisation that does and the expectation of the Church is that all Church Bodies will comply with the Privacy Act.

1.2.4 Entities that are subject to the Privacy Act are referred to as 'APP Entities'.

1.2.5 Some types of entities will be exempt from the application of the Privacy Act. This Manual discussed these in Paragraph 2.5.

1.3 Australian Privacy Principles

1.3.1 Church Bodies must comply with the APPs, which set minimum standards for the collection, use, disclosure, security, storage, access and correction of personal information. The APPs are summarised and explained individually in this Manual.

1.3.2 The Privacy Commissioner has released Guidelines on all the APPs. Although they are not legally binding, the Guidelines will assist with understanding how the Privacy Commissioner will interpret and apply the APPs. The APP Guidelines are available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/.

1.3.3 This Manual discusses the consequences of a breach and dealing with privacy complaints in relation to the APPs in Section 3.

2. WHAT INFORMATION DOES THE ACT COVER?

2.1 Regulation of 'personal information'

2.1.1 The Privacy Act regulates any type of information that is personal information (regardless of its source) that an APP entity collects for inclusion in a record or generally available publication. This includes health and other sensitive information that is also personal information as defined in the Privacy Act (see below). Personal information means information or an opinion that identifies an individual or allows them to be identified, whether the information or opinion is true or false and recorded in any form. It covers a range of information from contact details to photos, religion, bank payment details and medical records.

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

2.2 What is 'sensitive information'?

2.2.1 Sensitive information is a type of personal information that is given extra protection by the APPs (and health records legislation) and must be treated with additional care. It includes health information and also 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, or criminal record.

2.3 What is 'health information'?

2.3.1 Health information is a type of sensitive information and is broadly defined. 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 currently provided that is also personal information. Health information also includes personal information collected in the course of providing a health service.

2.3.2 For more details on the regulation of health information, see Section 18.

2.4 What is a 'record'?

2.4.1 The APPs only apply to personal information that a Church Body has collected and holds in a record. A 'record' includes a 'document' or an 'electronic or other device'. The definition is inclusive and therefore now covers a wide variety of material that might constitute a record.

2.4.2 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.

2.4.3 Some items are excluded from the definition of 'record'. The exclusions relevant to Church Bodies are:

(a) a generally available publication (e.g. a telephone directory); and

(b) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

2.5 Consent

2.5.1 Throughout the APPs there are provisions which require consent to be obtained. It is part of being open and transparent (see Section 4) 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 collection, access and use of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they consent to. The APP Guidelines provide that this practice of obtaining bundled consents has the potential to undermine the voluntary nature of the consent.

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 Church Bodies:

Small Business

A Church Body 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. However the Bishops' expectation is that all Church Bodies will comply with the Privacy Act. If a Church Body is to be treated as being related to or part of another Church Body, which does have a turnover of more than $3 million, then it will not be considered a small business.

One of the circumstances in which a Church Body will not be considered a 'small business' is where the Church Body both holds health information (other than in an employee record) and provides a health service. The Privacy Act defines 'health service' broadly. This exemption will mainly apply to Church Bodies that run aged care facilities that provide health services. It may also apply to Church Bodies that employ psychologists to counsel, for example, abuse victims.

Employee records

2.6.3 An act done, or practice engaged in, by a Church Body 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 organisation relating to the individual.

2.6.4 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.

2.6.5 Therefore generally all activity of a Church Body in relation to personal information it holds about its employees (eg uses, disclosures, security) will be exempt from the Privacy Act.

2.6.6 The employee records exemption does not extend to prospective employees, contractors, consultants or volunteers.

2.6.7 The Manual discusses issues around employee records in more detail at Section 19.

Transfers between related companies

2.6.8 The *Corporations Act* defines a related company or 'related body corporate' as either a holding company or subsidiary of another body corporate, or a subsidiary of a holding company of another body corporate.

2.6.9 Essentially, a related company refers to businesses that have a shared controlling interest. Particular issues arise in this regard for religious structures. It is unlikely, for example, that the Corporations Act would recognise a separately incorporated religious institute as a related body corporate of a Diocese. However, a Parish may consider itself to be similar to a related body corporate of the Diocese of which it is a part.

2.6.10 Under the Privacy Act, a company that is related to another company will be able to share and transfer personal information (but not sensitive information). However, those related companies must still comply with the APPs in relation to the shared personal information.

2.6.11 The primary purpose of the collection of the personal information of one body corporate will be deemed the same as that of the related body corporate that receives the information. Therefore the related body corporate may use and disclose the personal information for the same purposes as the original body corporate in accordance with APP 6 (see Section 7 below).

2.6.12 However, the related bodies corporate exemption applies only to the sharing of personal information (not sensitive information). Therefore, given that a large part of information that Church Bodies collect and use is sensitive information (such as health information and information about religious affiliations), this exemption may be of reduced significance.

3. APP BREACHES AND COMPLAINTS

3.1 Breach of the APPs

3.1.1 The breach of an APP by a Church Body will be an interference with an individual's privacy and a breach of the Privacy Act.

3.2 Complaints

3.2.1 Individuals may complain to Church Bodies if they think their privacy has been interfered with as they believe it has been handled inconsistently with/in breach of an APP.

3.2.2 Individuals must first complain to the relevant Church Body in writing. The Privacy Commissioner will generally refrain from investigating their complaint until a complaint has been made to the Church Body and the Church Body has an opportunity to resolve it.

3.2.3 APP requires Church Bodies to take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the Church Body's functions or activities that will enable it to deal with enquiries or complaints about its compliance with the APPs.

3.2.4 Church Bodies are also required to advise individuals in their privacy collection statement and Privacy Policy how they may complain about a breach of the APPs and how the Church Body will deal with that complaint.

3.2.5 If the Church Body cannot resolve the complaint, the individual may complain to the Privacy Commissioner, who may investigate the complaint. The Privacy Commissioner may resolve an upheld complaint by an order for redress of any loss or damage to the person whose privacy the Church Body has breached. This could include a compensation order.

3.2.6 If the entity does not comply with any orders made, the complainant can apply to have the order enforced in the Federal Court or the Federal Circuit Court.

3.3 Own motion investigations by the Privacy Commissioner

3.3.1 Notwithstanding the procedures described above, the Privacy Commissioner also has discretion to investigate, on his or her own initiative, an act or practice which may be an interference with privacy (i.e., a breach of the APPs) if the Privacy Commissioner thinks that it would be appropriate (e.g. even where no complaint has been made by the individual involved).

3.3.2 The Privacy Commissioner also has the power to assess whether an APP entity is complying with the APPs.

3.4 Penalties

3.4.1 The Commissioner may accept written undertakings from an entity that it will take or refrain from taking specified actions to comply with the Privacy Act or take specified actions to ensure that the APP entity does not interfere with the privacy of an individual in the future. If an entity breaches an undertaking, the Commissioner can apply to the Federal Court or Federal Circuit Court for orders directing the APP entity to comply with its undertaking or to compensate anyone who has suffered loss or damage because of the breach of the undertaking or for any other order that the court considers appropriate.

3.4.2 Additionally, the Privacy Commissioner has the power to seek pecuniary penalties of up to $340,000 for individuals, and $1.7 million for APP entities in circumstances where there has been a serious or repeated interference with privacy.

3.4.3 The Privacy Commissioner has indicated that although the complaints process is designed to ensure that most complaints can be resolved through conciliation and mediation rather than through the courts, pecuniary penalties will be sought in appropriate circumstances.

PART 2 – THE AUSTRALIAN PRIVACY PRINCIPLES

This Part sets out a detailed commentary on each of the APPs.

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

4.1 Open and transparent management of personal information (APP 1)

Requirement:
A Church Body must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its functions or activities that will ensure that the Church Body complies with the APPs and a registered APP code (if any) that binds it, including how to deal with inquiries and complaints. (Section 3 dealt with complaints.)

4.1.1 A Church Body must plan in advance as 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 as are reasonable in the circumstances' to implement practices, procedures and systems relating to its functions and activities to achieve this.

4.1.2 What constitutes 'reasonable steps' will depend on the circumstances. For example, a small Parish would not be required to take the same steps or implement the same systems and procedures as would be expected of a large Archdiocese.

4.1.3 As part of complying with the APPs, a Church Body will also be required to consider privacy obligations when planning any new systems. This is part of a move towards a 'privacy by design' approach to compliance - that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception.

4.1.4 The significance of this principle is that:

(a) this is an overarching requirement and therefore applies to compliance with all of the APPs;

(b) the Privacy Commissioner has the power to investigate compliance with APP 1, that is whether an APP entity is properly managing personal information, even where there is no breach of an APP; and

(c) if the Privacy Commissioner found an entity to be in breach of another APP, it is quite possible that it would also find it to be in breach of APP 1.

4.2 How to comply:

4.2.1 The Church Body should:

(a) plan in advance how it will handle personal information in compliance with the APPs prior to collecting and processing any personal information;

(b) train and communicate to staff, contractors, volunteers and clergy information about the Church Body's information handling policies and practices;

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

(d) develop information to explain its policies and procedures; and

(e) establish procedures to identify and manage privacy risks and compliance issues, including designing and implementing systems or infrastructure for the collection and handling of personal information by the Church Body.

4.3 Privacy Policy (APP 1.3-1.6)

4.3.1 Requirement:

A Church Body must have a clearly expressed and up-to-date policy about the management of personal information by the Church Body (APP 1.3) that 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 Church Body will deal with that complaint; and

(f) whether the Church Body 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).

4.3.2 Requirement

A Church Body 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. If the Church Body has a website, it will usually make its Privacy Policy available on the website. (APP 1.5)

4.3.3 Requirement

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

4.3.4 It is important that the Church Body make its Privacy Policy widely available (including to employees and volunteers).

4.4 How to comply:

4.4.1 Prepare a Privacy Policy (based on the template included at Annexure 2), which expresses, in plain language, the Church Body's policy or policies on its management of personal information.

4.4.2 Keep the Privacy Policy 'up-to-date' as a 'living document' and review it regularly (for example, diarise an annual review).

4.4.3 Use the Privacy Policy not only to explain how the Church Body handles personal information, but also to guide staff on privacy standards and to ensure consistency in the Church Body's approach to information privacy.

4.4.4 Make the Privacy Policy available on the Church Body's website (if it has one) and on a noticeboard, and draw attention to it whenever personal information is collected.

4.5 Training staff

4.5.1 Achieving compliance will also depend on the conduct of the Church Body's staff who must understand its privacy obligations. This can be done by:

(a) circulating the Privacy Policy to staff and requiring them to read it and acknowledge receipt;

(b) informing staff of the requirements of confidentiality and extending this obligation contractually where necessary; and

(c) holding internal seminars and workshops.

4.6 Do's and Don'ts

DO, if asked, inform people about the type of personal information that is being collected about them and why.

DO encourage staff to read the Church Body's Privacy Policy.

DO make the Privacy Policy easily accessible.

DO ensure that the Church Body follows its requirements in relation to the collection, use and disclosure of personal information.

DO ensure staff refer all queries about the Privacy Policy to the Church Body's privacy officer or to someone responsible for privacy compliance.

5. ANONYMITY AND PSEUDONYMITY (APP 2)

5.1 Anonymity and Pseudonymity

5.1.1 Requirement:

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

(a) the Church Body 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.

5.2 Comment

5.2.1 The Privacy Commissioner considers that unless there is a good practical or legal reason to require identification, a Church Body must give people the option to interact anonymously.

5.2.2 Anonymity is an important element of privacy. However, in some circumstances, it will not be practicable to engage with an individual anonymously. In other circumstances, there will be legal obligations that require identification of the individual. This principle is not intended to facilitate illegal activity.

5.3 How to comply:

5.3.1 Make individuals aware of the circumstances in which they are able to deal with the Church Body anonymously or when they can use a pseudonym instead of their real name. This can be done through information in the privacy policy and privacy collection statements, and when the Church Body is dealing with the individual.

5.3.2 Identify circumstances where:

(a) a law or order of a court or tribunal may require or authorise the Church Body to only deal with identified individuals (e.g. if providing assistance to a suspected victim of child abuse, whose injury is covered by a mandatory reporting requirement); or

(b) it would be impracticable to deal with an individual who is not identified (e.g. as part of a dispute resolution process).

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

6.1 Collection

6.1.1 The APPs differentiate between and have rules that apply to the collection of information that is 'solicited' and 'unsolicited'. 'Solicited information' is information that the Church Body has asked the individual or a third party to provide.

6.1.2 Requirement:
A Church Body 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).

6.2 Sensitive Information (APP 3.3 and 3.4)

6.2.1 Requirement:
In general, a Church Body must not collect sensitive information about an individual, unless it has consent or one of the following exceptions applies.

(a) collection is required by law, which includes the common law duty of care;

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

(c) the sensitive information is health information and the Church Body has collected it in circumstances that is prescribed as a permitted health situation. (See Section 18.3 for more information about situations relating to collection of health information).

6.2.2 Sensitive information is personal information that is given extra protection by the APPs (and health records legislation) and must be treated with additional care. It includes health information and also 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, or criminal record.

6.2.3 In a large number of cases, sensitive information, including health information, will be provided to the Church Body by the individual (or their guardian), so it is clear that the Church Body has consent to collect that information.

6.2.4 However, on some occasions the Church Body may receive sensitive information from third parties in circumstances where the Privacy Act also permits that collection. For example, a Parish school may advise a Parish about health issues relating to a child who is under the care of the Parish while preparing to receive a sacrament, in order for the Parish to exercise its duty of care. This collection by the Parish would be authorised by law.

6.3 Comment

6.3.1 The Privacy Commissioner interprets 'reasonably necessary' in a practical sense. If a Church Body cannot effectively pursue a legitimate function or activity without collecting the personal information, then it would ordinarily be deemed 'necessary' for one or more of its functions or activities. A Church Body should not collect information on the 'off-chance' that it will be of some use in the future.

6.3.2 The collection of personal information, which law requires, would also be deemed as being 'necessary' for one or more of a Church Body's functions or activities.

6.4 How to comply:

6.4.1 Review the types of personal information that the Church Body collects to ensure it is reasonably necessary for one or more of the Church Body's functions or activities.

6.4.2 Ensure that the Church Body collects sensitive information only where there is consent or where an exception applies.

6.5 Lawful and fair collection (APP 3.5)

6.5.1 Requirement:

A Church Body must collect personal information:

(a) only by lawful and fair means; and

(b) not in an unreasonably intrusive way.

6.6 Comment

6.6.1 Generally, 'fair' means without intimidation or deception. For example, covert collection will usually be considered as unfair collection.

6.6.2 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.

6.7 How to comply:

6.7.1 Regularly review the Church Body's collection procedures. Particular acts and practices of collection should be identified and monitored for instances (whether systemic or by particular individuals) of unfair, unlawful or unreasonably intrusive collections.

6.7.2 Any complaints concerning the methods of collection should be part of this monitoring process.

6.7.3 Be careful to consider and re-consider the context in which personal information is collected. Always be mindful that Church Bodies should collect personal information and sensitive information discretely.

6.8 Privacy collection statement - ensuring the individual is fully aware of collection (APP 5.1)

6.8.1 Requirement:

At or before the time (or, if not practicable, as soon as practicable after) a Church Body collects personal information about an individual from the individual, the Church Body 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 Church Body'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 (including other Church Bodies);

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

(h) that the Privacy Policy sets out how complaints may be made, 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.

6.9 Comment

6.9.1 Deciding on whether a Church Body should make individuals aware of the required matters 'at or before the time of collection' will depend on the circumstances. Church Bodies can do this after the collection of the information if there are practical problems in doing so before collection.

6.9.2 APP 5.1 has a 'double reasonableness' provision. A Church Body 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 any of these matters are obvious, irrelevant or can be easily located (e.g. the identity of the Church Body) it may not be necessary to inform people of that matter in a collection statement.

6.9.3 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 Church Body makes available to an individual the matters contained in APP 5.1 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.

6.9.4 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 Church Body in providing that information.

6.9.5 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 the Church Body is going to do with their personal information. Church Bodies do not have to describe internal purposes that form part of normal business practices, such as auditing, business planning or billing.

6.9.6 Taking 'reasonable steps' to inform an individual about usual disclosures would ordinarily mean either giving general descriptions of sets of people and entities to which the

information may be disclosed (for example, a Parish may often disclose information to the responsible Diocese).

6.9.7 A Church Body does not need to mention disclosures that the APPs permit, but in practice happen only rarely.

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

6.9.9 A Church Body need not describe all possible consequences of not providing personal information, only significant and unobvious consequences.

6.10 How to comply:

6.10.1 Take a common sense and pragmatic approach when complying with APP 5.1 and APP 5.2. The requirements under the APPs 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.

6.10.2 Tailor the template standard collection notice at Annexure 2 to cover the Church Body's usual collection practices or any specific or unique collections, and ensure that it covers the matters listed in APP 5.1 concerning how any personal and sensitive information collected from the individual about him/herself or a third party would be dealt with.

6.10.3 Where the Church Body collects personal and sensitive information from those who have not seen collection notices (e.g. third parties) or where the collection notices do not cover a particular situation, then the Church Body should consider, with reference to the APPs and the APP Guidelines, whether it needs to take additional steps to comply with APP 5.1 and notify those people of the matters set out in APP 5.2. In particular, where a Church Body intends to use a film including a child or a child's photo in a public forum (such as on television or on social media, such as Facebook and Flickr) the Church Body should seek permission from the child and/or the child's parent or guardian as appropriate.

6.11 Collection through surveillance

6.11.1 If a Church Body has implemented surveillance systems, including closed circuit television or monitoring of computer systems, networks and facilities, it should advise people interacting with the Church Body or using those systems that they might be monitored. If a person is being monitored, even through their computer use, personal information may be collected.

6.11.2 Specific legislation in certain States and Territories governs the surveillance and monitoring of persons on Church property. For example:

(a) in New South Wales, specific legislation requires employers to notify their employees in advance that their computer use will be monitored;

(b) additionally, legislation in New South Wales, Queensland, Victoria and Western Australia, requires employers who use surveillance devices such as security cameras, closed circuit television or telephone monitoring to obtain the express or implied consent of those persons to do so. The Church Body could obtain this consent via a contract of employment, through policies or notices, or by using signs in areas where such surveillance occurs.

6.11.3 The Church Body should provide anyone using the system (such as employees, volunteers, contractors and clergy) with a computer usage policy. Ideally, they should provide to the Church Body written acknowledgement that they have received that policy.

6.11.4 Additionally a Church Body should notify individuals of any other instances of surveillance in the contract of employment, through policies or notices, or with signage in areas where it engages in surveillance.

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

6.12.1 Requirement:
Where reasonable and practicable to do so, personal information must only be collected directly from the individual.

6.13 Comment

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

6.13.2 It is apparent that it will not always be reasonable and practicable to collect personal information from the individual directly. In most scenarios, the individual concerned is aware of an indirect collection and consent can be inferred. However, this may not always be the case.

6.13.3 Where a job applicant is aware that a referee is providing information about them to a Church Body (therefore indirect collection), a Church Body can imply that they consent to that indirect collection. However, if the Church Body collects personal information from a referee or third party without the applicant's knowledge (e.g. the job applicant's current employer), the Church Body should advise the individual that they will be collecting, or have collected, the information.

6.13.4 Church Bodies should note however, that 'collection' only relates to information that is contained in a record. Information obtained from an inquiry, which is not recorded, does not constitute a record and therefore no collection occurs.

6.14 How to comply:

6.14.1 There may be some circumstances in which a Church Body should only collect information directly from the individual. A Church Body should consider these circumstances on a case-by-case basis.

Example:
Where it is likely that the information is incorrect, (e.g. the source is unreliable) then the Church Body collecting the information should endeavour to contact the individual concerned to check whether the information is accurate. It will not always be reasonable and practicable to do this. For example, the individual concerned may be the subject of an allegation about an unlawful activity and approaching that person may prejudice the investigation.

6.15 Collection, use and disclosure with third parties and contractors (APP 3.6 and APP 6)

6.15.1 Where the Church Body engages a contractor or third party, the following may occur:

(a) the Church Body collects personal information from a contractor or third party;

(b) the Church Body discloses personal information to a contractor or third party; or

(c) a contractor uses or discloses personal information on behalf of the Church Body.

6.16 How to comply:

6.16.1 Specifically require the contractor, in a written agreement, to keep personal information confidential that it provides about individuals in the course of providing the service to the Church Body and only use it for the purposes of the Church Body.

6.17 Collecting sensitive information with consent

6.17.1 The Church Body would normally need clear evidence that an individual had consented to it collecting sensitive information. 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.

6.18 Collecting sensitive information without consent

6.18.1 In most situations Church Bodies will collect sensitive information with consent on the basis that it has been provided to them directly by the individual, their guardian or other responsible person, or a person authorised by the individual such as a doctor.

6.18.2 However, occasions may arise where Church Bodies collect sensitive information from third parties without consent. The Privacy Act permits this where it is required or authorised under law (this includes a duty of care) or it is impracticable to obtain consent and it is reasonably necessary to lessen or prevent a serious threat to the life, health or safety of the person or to public health or safety. It may also be necessary when investigating a suspected case of child abuse where there is a legal obligation to make inquiries without disclosing that there is an investigation.

6.19 How to comply:

6.19.1 Ensure that a Church Body collects sensitive information only with consent, where required or authorised by law, or where another exception applies. Comments on the issue of capacity to consent are contained are in Paragraph 15.1. A guardian or other responsible person may be able to be give consent, where needed, if the individual lacks capacity.

6.19.2 Ensure that you also meet the requirements of APP 3 and APP 5. Make sure that the collection is reasonably necessary for one or more of the Church Body's functions and activities (APP 3.3(a)(ii)), and take such steps (if any) as are reasonable in the circumstances to notify the individual of the matters in APP 5.2 (APP 5.1). There may be some instances where notification should not be given or is unnecessary.

6.19.3 Pre-empt situations where sensitive information is collected from third parties, by making the individual whose information is collected aware that their sensitive information is likely to be collected, and to obtain their consent to such collection. A standard collection notice (see the template at Annexure 2) can cover the collection of sensitive information in, however it may be appropriate on some occasions to get specific consent and give a specific collection notice.

6.19.4 In some instances, there is collection of sensitive information due to a legal obligation to collect such information.

Example:
Examples of collection as required by law include:

(a) certain criminal record checks and/or working with children checks (e.g. as required under child protection laws in some States);

(b) information required to administer the sacraments; and

(c) laws which require verification of an individual.

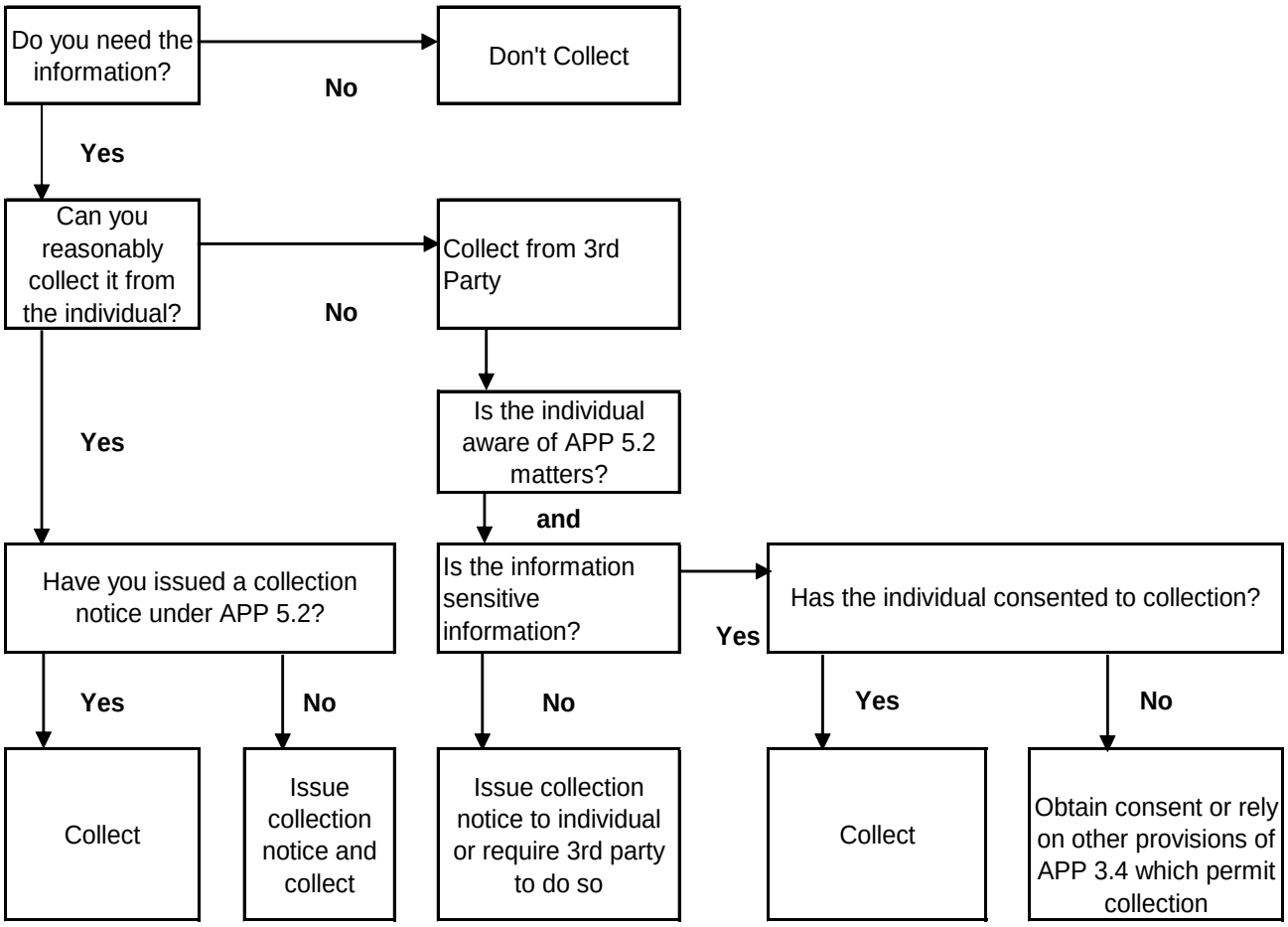
6.19.5 Where law requires collection of sensitive information, APP 3.4(a) will permit the collection of sensitive information without consent. However, APP 5.1 will continue to apply and it may be necessary to inform the individual that this information is being collected.

6.19.6 Where practicable, clearly identify sensitive information as being such in any records. This practice would help ensure that the persons handling the information recognise the extra confidentiality and security that should be afforded to sensitive information.

6.19.7 Information about religion, racial and ethnic origin (also sensitive information) is in a different category. If this information is collected from the individual, then consent can be implied. However, if this information is collected from a third party, permission should first be sought.

6.19.8 The table at Section 6.20 below illustrates the steps a Church Body should follow in deciding whether it can collect personal and sensitive information.

6.20 Collection Compliance Steps



6.21 Unsolicited Personal Information (APP 4)

6.21.1 Requirement:

(a) If a Church Body receives unsolicited information it must within a reasonable period determine whether it could have collected that information under APP 3.

(b) 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.

6.21.2 Church Bodies are required 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 Church Body'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 to which Paragraph 6.2 refers.

6.21.3 On many occasions, it is likely that a Church Body will receive unsolicited personal information verbally. In order to meet the requirements of APP 4, Church Bodies should adopt a rule that it should not make any notes of unsolicited personal information received verbally unless it needs it and, in the case of sensitive information, an exception for collection without consent exists.

Example:
A member of the congregation advises the priest that she understands that another parishioner was intoxicated at a party they both attended.

This is not information that is relevant to the Church Body's operations and should not be collected.

6.22 Do's and Don'ts

DO only collect personal information that the Church Body requires to carry out its functions and activities.

DO identify the Church Body and its contact details when collecting personal information.

DO inform individuals that they can access their personal information, subject to the requirements of the Privacy Act.

DO inform individuals of any plans to disclose their personal information to others.

DO consider, and notify individuals of, all the reasons for which you are collecting their personal information.

DO take reasonable steps to ensure that, when collecting personal information, the Church Body makes individuals aware of the matters listed in Section 6.8.1 unless it is obvious or they would already know.

DON'T collect personal information from someone about another individual (e.g. next of kin details) unless it is unreasonable or impracticable for you to contact the individual directly.

DON'T collect unsolicited information if it is not reasonably necessary for a function or activity of the Church Body.

6.23 Additional Do's and Don'ts for sensitive information

DO only use sensitive information for the purposes for which it was disclosed.

DO obtain consent if you collect sensitive information unless an exception applies.

DON'T collect sensitive information unless it is necessary.

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

7.1 Use and Disclosure

7.1.1 Requirement:
A Church Body 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) with the individual's consent (APP 6.1(b));

(c) for a secondary purpose 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));

(d) where required or authorised by or under law (APP 6.2(b));

(e) where the Church Body reasonably believes that the use or disclosure is necessary to prevent threats to life, health or public safety (APP 6.2(c));

(f) where the Church Body 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));

(g) where the Church Body reasonably believes the use or disclosure is reasonably necessary to assist with locating a person reported as missing (APP 6.2(c)).

7.2 Primary and related purpose of collection

7.2.1 Where the Church Body collects personal information directly from the individual, the context in which the individual gives the information to the Church Body will help identify the primary purpose of collection. When an individual provides, and the Church Body collects, personal information, they usually do so for a particular purpose – for example, for admission to an aged care facility operated by the Church Body, to apply to become a volunteer or employee, or to receive a sacrament. This is the 'primary' purpose of collection, even if the entity has some additional purposes in mind.

7.2.2 How broadly a Church Body can describe the primary purpose will need to be determined on a case-by-case basis and will depend on the circumstances.

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

7.2.4 *Related and directly related purposes within reasonable expectations*
A Church Body can also use and disclose the personal information for a related or, if it is sensitive information, for a directly related purpose, for which the individual would reasonably expect their information to be used or disclosed. 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 for collection.

7.2.5 *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 activity involved would expect.

7.2.6 *Factors to consider*
When thinking about whether a use or disclosure falls within the primary purpose or a related or directly related purpose within the individual's reasonable expectations, a Church Body 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 Church Body has given about why it is collecting the individual's information (for example under APP 1.4 and 5.2);

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

(e) any duties of care or other professional obligations a Church Body might have (although care would be needed if these were not within the person's reasonable expectations).

7.2.7 *Secondary use and disclosure with consent (APP 6.1(a))*
A Church Body may also 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 Church Body. If the Church Body's use or disclosure has serious consequences for the individual, the Church Body 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 to have given their consent on that basis. In such situations, it would ordinarily be more appropriate for the Church Body to seek express consent.

7.3 How to comply:

7.3.1 Use an appropriately adapted version of the template collection statement at Annexure 2 to help overcome any potential for confusion regarding the purposes for which the information can be used.

7.3.2 Consider any forms through which personal information is collected to ensure that they include an appropriate collection notice.

7.4 Use or disclosure required by law (APP 6.2(b))

7.4.1 The Privacy Act does not override specific legal obligations relating to use or disclosure of personal information. 'Law' includes Commonwealth, State and Territory legislation, as well as common law. If law requires an entity to use or disclose personal information, it has no choice and it must do so. If an entity is authorised by law to use or disclose personal information it means the entity can decide whether to do so or not.

7.4.2 For example, in New South Wales, there is specific legislation that authorises disclosure of personal information for certain child protection purposes.

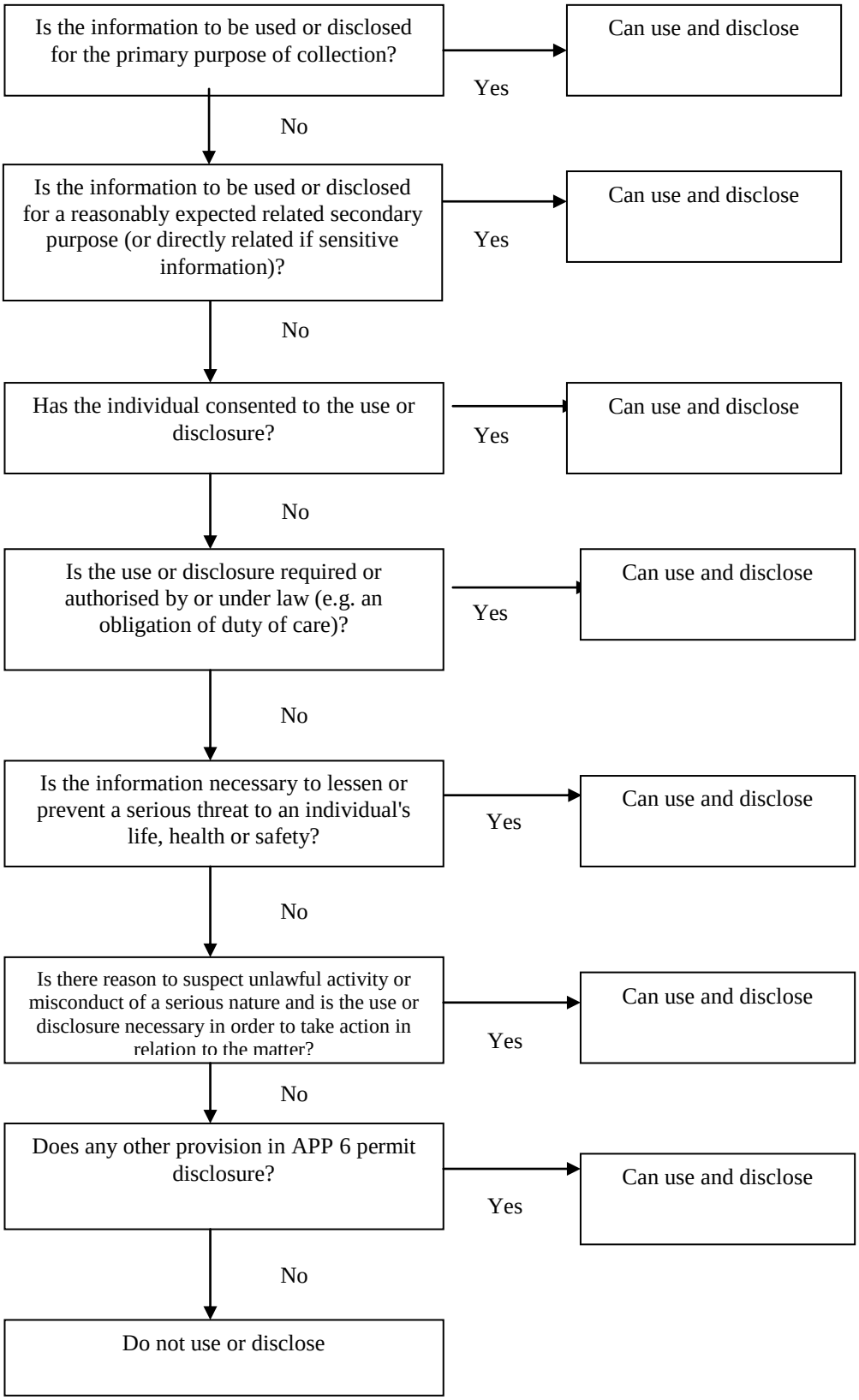
7.5 How to comply:

7.5.1 Where a disclosure is required because of a duty of care owed to an individual, then this may be done under APP 6.2(b) without the individual's consent. Similarly, where there is

a legislative requirement to disclose information this may be done under APP 6.2(b) without the individual's consent.

7.5.2 The table at Section 7.6 below illustrates what steps should be taken by the Church Body in deciding whether it can use or disclose personal and sensitive information.

7.6 Use & Disclosure Compliance Steps



7.7 Do's and Don'ts

DON'T disclose personal information unless with consent, for the primary purpose of collection or for a reasonably expected related secondary purpose of collection (or *directly* related secondary purpose in the case of sensitive information) or where another exception applies, such as exercising duty of care.

DO make a written note of use or disclosure of personal information if used or disclosed under an exception in APP 6.2.

8. DIRECT MARKETING (APP 7)

8.1 Direct Marketing

Requirement:

A Church Body 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 Church Body 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, of which the individual has not availed him or herself (APP 7.2).

Scenario 2:

(d) either:

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

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

(e) either:

  (i) the individual has consented; or

  (ii) it is impracticable to obtain consent; and

(f) there is a simple means by which the individual can request not to receive direct marketing; 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).

Requirement:

If a Church Body 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 source of the information received (unless it is impracticable or unreasonable to do so).

Requirement:

A Church Body may not use or disclose sensitive information for direct marketing unless the individual has consented (APP 7.4).

Requirement:

The *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth) (**DNCR Act**) will displace the requirements of APP 7, to the extent these Acts apply to the direct marketing practices of Church Bodies via electronic commercial direct marketing (Spam Act) or telemarketing (DNCR Act). However, electronic messages, telemarketing calls and marketing faxes sent by Church Bodies that are registered as charities with the Australian Charities and Not-for-profits Commission (**ACNC**) will generally be exempt from the Spam Act and DNCR Act. Consequently, if communications are exempt from the Spam Act and/or the DNCR Act, they will need to comply with APP 7.

8.2 Comment

8.2.1 'Direct marketing' involves the Church Body's direct communication with a person to promote the sale of goods and services to that person (which means it will generally involve a payment or financial benefit of some kind to the Church Body). A range of methods including mail, telephone, electronic mail or Short Message Service could deliver the direct marketing communication. A fundraising campaign, an invitation to a conference or an invitation to subscribe to a magazine are examples of direct marketing campaigns by a Church Body.

8.2.2 A discrete APP now addresses direct marketing separately, so APP 6 does not apply. This is because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing.

8.2.3 The principle distinguishes between individuals, such as existing or previous parishioners, who have been in contact with a Church Body, 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 the Church Body. This is because those individuals would be less likely to expect the Church Body to use or disclose their information for direct marketing purposes.

8.2.4 A Church Body may use and disclose non-sensitive personal information for direct marketing where, among other things, the individual would reasonably expect the Church Body to use or disclose their information for direct marketing, and there is a simple means by which the individual can request not to receive direct marketing material. A Church Body may not use sensitive information for direct marketing unless it has obtained consent to do so.

8.2.5 *'Reasonable expectation'*
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 any collection notice provided at the time;

(b) the way a Church Body communicates with an individual;

(c) the previous types of communications between a Church Body and an individual;

(d) how often the Church Body is in contact with an individual and the purpose of the contact; and

(e) the duration of a Church Body's relationship with an individual

A Church Body would generally consider the question of 'reasonableness' at the time of the proposed use of the personal information for direct marketing – not the time it collected the personal information.

8.2.6 *'Impracticable to obtain consent*'
The APP Guidelines state that to determine whether it is 'impracticable' to obtain consent will depend on a number of factors, including the time and cost involved in seeking consent. However, an organisation 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.

8.2.7 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 direct marketing at the time it collects the personal information. In order

to rely on this consent, the organisation must be satisfied that it is still current at the time of the use or disclosure.

8.2.8 Where an organisation did not obtain the individual's consent at the time of collection, it must obtain the consent of the individual for the proposed use or disclosure, unless it is impracticable to do so. In that case, the organisation should assess whether it is impracticable to obtain consent at the time of the proposed use or disclosure.

8.2.9 *Disclosure/sharing of personal information for direct marketing*
If Church Bodies are to be treated as if they were related bodies corporate, as discussed at Section 2.6 above, they can share personal information (other than sensitive information) without breaching the APPs. However, those related Church Bodies must still comply with the APPs in relation to the shared personal information. It will therefore depend on the circumstances of the collection by the original Church Body as to whether a related Church Body is then permitted to use and/or disclose that personal information for direct marketing.

8.2.10 If the Church Bodies cannot be considered to be related bodies corporate, then:

(a) the disclosing Church Body will only be able to disclose personal information for the purpose of direct marketing in accordance with the provisions of APP 7 (Scenario 1); and

(b) the collecting Church Body will need to comply with APP7 (Scenario 2) and APP 5 in relation to the use of the information for direct marketing and notification of the collection.

8.3 How to comply:

8.3.1 Identify whether an individual would reasonably expect their personal information to be used for direct marketing purposes, either because they have been provided with a collection statement which tells them that their information may be used or disclosed for this purpose, or because they would otherwise be aware that their information may be used for such a purpose (e.g., a regular donor may have a reasonable expectation that they would receive direct marking communication regarding fundraising efforts).

8.3.2 However, if a Church Body is to send direct marketing communications to people to whom it has not provided the 'standard collection notice' or are not otherwise aware of its contents, then the Church Body may need to rely on APP 7.3 to send the direct marketing communications.

8.3.3 If relying on APP 7.3, ensure each direct marketing communication includes a simple means by which the individual may request not to receive direct marketing communications, and a prominent 'opt-out' statement, which the Church Body should bring to the individual's attention. An example would be:

> Direct marketing opt-out
>
> We may use and share your personal information with [***insert usual examples or other Church bodies***] to send you further fundraising/direct marketing communications. If you do not wish to receive such communications [**OR** either some or all of these communications from us*], please tick the box[es*] below and return this [***form***] to [***us***].
>
> ☐ No, I do not wish to receive fundraising/direct marketing communications.
> [*_**Use two boxes if giving option to make separate elections - one for fundraising and one for direct marketing communications**_].

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

9.1 Cross-border Disclosure

9.1.1 Requirement:
If a Church Body 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 still 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.

9.1.2 A Church Body will not be required to comply with the above provision in some limited circumstances, including where:

(a) it 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; 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) law requires or authorises the disclosure.

9.2 How to comply:

9.2.1 If the Church Body is likely to disclose personal information overseas, it must have procedures in place for ensuring that it addresses the requirements of APP8.

9.2.2 Before disclosing the personal information, a Church Body will need to take 'reasonable steps' if an exception does not apply, to ensure the overseas entity handles the information in accordance with the APPs.

9.2.3 Examples of when a Church Body in Australia might disclose personal information (which does not include statistics) overseas are when it:

(a) liaises with a Church Body located overseas in relation to a transferring member of clergy;

(b) where an individual requests that their baptismal records, or records of other sacraments, be sent to a Church Body located overseas; or

(c) where Australians register to attend a convention overseas.

9.2.4 Compliance with APP 8 can be achieved if the Church Body:

(a) enters into a contract with each intended recipient of the information which requires the recipient 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 continues); 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 being told that the protections provided under the APPs may not apply. If Church Bodies wish to rely upon this exception, they should seek specific advice on the form of notice to use and they will have to draft specifically the consent to meet the particular situation.

9.2.5 If a Church Body needs to disclose personal information for a particular purpose, such as where an individual has requested that their information be sent to a Church Body located overseas, the Church Body could seek a consent for that particular disclosure. An example would be:

Consent to overseas disclosures

> I/We consent to the disclosure of our/the-personal information of [***name/s***] to [***identify recipient or class of overseas recipients***] for the purpose of [***insert purpose of the disclosure, e.g. enabling the individual to receive a sacrament in an overseas parish***].
>
> * I/We acknowledge that we are aware that the overseas recipient may not be bound by laws which give the same level of protection for personal information as the Privacy Act 1988 (Cth) and agree the Church Body will not be responsible for any breach of privacy by [***the recipient or class of overseas recipients***].
>
> *If applicable

9.3 Using cloud storage providers

9.3.1 Some Church Bodies may also be storing personal information in the 'cloud'. Cloud providers may be storing the information offshore, sometimes in multiple or changing locations. It is important that Church Bodies are aware of the practices of the cloud provider and enter into appropriate arrangements to limit their exposure should a data breach occur.

9.3.2 The use of a cloud service provider by a Church Body may trigger the requirements under APP 8. However, the APP Guidelines provide that where a Church Body provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the Church Body 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 information is provided for the limited purpose of storing and managing the information;

(b) the contract between the Church Body and the overseas cloud service provider binds the provider not to use or disclose the personal information except for the limited purpose of storing and managing the information;

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

(d) the contract between the Church Body and the cloud service provider gives the Church Body effective control of the information.

9.3.3 As some have questioned this interpretation in the APP Guidelines, it would be prudent to include a reference to using an offshore cloud service for storage in relevant collection notices.

9.3.4 If a Church Body is using an offshore cloud service for more than storing and managing personal information, the Church Body will also be required to advise people in collection

notices that their personal information may be sent offshore and, if known, to which countries.

9.3.5 It is strongly suggested that if a Church Body 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 seek also an indemnity from the recipient to protect the Church Body against claims in the event of a data breach.

9.4 Do's and Don'ts:

DO take care when disclosing information overseas.

DO investigate the privacy obligations of overseas recipients of personal information, rather than simply taking their word for it, if you intend to rely upon the Reasonable Belief Defence.

DO ensure that 'cloud' providers offer appropriate undertakings, warranties and indemnities.

DO advise people if their information will or may be sent offshore and if practicable when it will be sent.

DO obtain consents for one-off transfers of information where it is practicable to do so.

10. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS (APP 9)

10.1 Identifiers

10.1.1 Requirement:
APP 9 requires that identification devices (the unique combination of letters and numbers) provided by a Commonwealth/State/Territory government agency (or the agency's contracted service provider), such as a Medicare number, a Social Security number, a drivers licence number or a tax file number, cannot be:

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

(b) used or disclosed unless it is reasonably necessary to verify identification of the individual or to fulfil its obligations to an agency, Commonwealth/State/Territory government agency or other limited circumstances permitted by APP9.

10.2 Comment

10.2.1 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.

10.2.2 For these reasons tax file number legislation already restricts the way an organisation can collect, use or disclose a tax file number and there are special rules issued under the Privacy Act in relation to their handling.

10.2.3 APP 9 does not apply to an individual's name.

10.3 How to comply:

10.3.1 Ensure that the Church Body does not adopt, as its own identifier of an individual, one that has already been assigned to the individual by a government agency.

10.3.2 In addition, when using or disclosing identifiers, such as a Medicare number, ensure that APP 9 permits any use or disclosure. The Church Body should ensure that workers are not able to enter a person's Medicare or employee's tax file number into a database in order to retrieve their record.

10.4 Do's and Don'ts:

DO only use identifiers that the Church Body has created to identify individuals.

DON'T collect or use agency or authority identifiers, such as an individual's Medicare number or passport number, unless it is necessary to fulfil a legal obligation or it is necessary to verify a person's identity.

11. DATA QUALITY (APP 10)

11.1 Data Quality

11.1.1 Requirement:
A Church Body 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 A Church Body should establish procedures for updating records, passing on changes, deleting records that are no longer used or required and contacting entities to which it has disclosed the records.

11.2 Comment

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

11.2.2 The APPs now 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 Church Body to inquire about the purpose before making the disclosure.

11.2.3 Reasonable steps to confirm the accuracy, completeness and currency of the personal information a Church Body collects only needs to be taken at the time it collects, uses or discloses the information. It is important that a Church Body check information at the times when it is to use or disclose it, to determine if it is not accurate, complete, up-to-date or relevant.

11.3 How to comply:

11.3.1 Establish standard procedures to ensure that the personal information the Church Body collects, uses or discloses is accurate, complete and up-to-date.

11.3.2 Keep in mind that the reasonableness of the measures taken will 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) the source of information.

11.3.3 The Church Body is required to check all records of personal information for accuracy, completeness, relevancy and currency only when it is to use or disclose the information.

11.3.4 Procedures should be adopted to ensure that:

(a) records containing sensitive information such as health information be checked for accuracy before being used or relied upon;
(b) there is a regular audit of all records of personal information held, whereby records that are not used or required are disposed of and inaccurate records updated;
(c) if records are to be disclosed, there is a check on relevance of the records disclosed and their accuracy;
(d) records are de-identified or destroyed when no longer needed by the Church Body; and

(e) either in conjunction with the 'regular audit' or otherwise, a periodic 'mail-out' is made to the information provider, providing an opportunity to update, and ensure the accuracy of, their personal information.

11.4 Sharing personal information

11.4.1 Where personal information is shared between Church Bodies (such as between a Parish and the relevant Diocese), the disclosing and receiving Church Body should keep records as to whom the personal information was disclosed to/collected from. Once either Church Body becomes aware of any change in the personal information then that Church Body may then pass on such changes and corrections to the other Church Body. This will help ensure that the information held by both Church Bodies is consistent and remains accurate and up-to-date. See Paragraph 2.5 regarding the related companies' exemption.

11.4.2 What procedures are put in place in this regard will likely depend upon the size of the Church Body.

11.5 Do's and Don'ts

DO be familiar with the Church Body's systems to ensure accurate and up-to-date personal information is kept.

DO consider the age of personal information, and whether the information is likely to change (e.g. an address is more likely to change than a name), in determining whether it is likely that the information is inaccurate, incomplete or out-of-date.

DO, when passing personal information internally or to another Church Body, notify the other party of the age of the information if this is likely to affect its accuracy and currency.

DO consider the impact if the information is incomplete, inaccurate or out-of-date (e.g. health information) and take appropriate steps.

DO investigate any clear inconsistencies with personal information held (e.g. a member of clergy is recorded as being only 17 years old).

DO consider whether the information was collected directly from the individual and whether it is a reliable source.

DO give the individual a chance to comment on the information provided, if reasonable and practicable to do so.

DO, where practicable, check personal information with existing records collected for the same or a related purpose to see whether it is consistent, accurate and up-to-date before using or disclosing personal information.

DO try to provide individuals with user-friendly ways to update their information.

DO keep records accurate by notifying any other Church Bodies from/to which personal information is collected/disclosed of any changes to the information, and keep a record of such notification.

DO check with a person to whom information is to be disclosed about the purpose of the disclosure, if this is not clear.

DON'T continue to use information you believe to be out of date or inaccurate.

12. DATA SECURITY (APP 11)

12.1 Security of Personal Information

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

12.1.2 As noted previously, Church Bodies may collect large amounts of personal information ranging from names and addresses to health information and credit card details. The unauthorised disclosure of or access to this information can have serious consequences, both personal and financial. Increasingly sophisticated methods of storing and accessing stored information have paradoxically also provided greater opportunities for misuse.

12.1.3 The level of security should be in proportion to the risk to the individual if their personal information is not secure. Therefore, a Church Body must take extra care 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.

12.1.4 The APPs have now introduced a requirement that reasonable steps must be taken to prevent 'interference' with personal information. This is intended to cover the unlawful accessing of electronic databases.

12.1.5 A difficulty for Church Bodies is that they usually do not have single entry points for data or one consistent system of storage and access. In dealing with security, Church Bodies need to consider this factor.

12.1.6 The Office of the Australian Information Commissioner issued a Guide to Information Security: 'Reasonable Steps' to Protect Personal Information (the 'Security Guide') in April 2013, which can be accessed at:
http://www.oaic.gov.au/publications/guidelines/privacy_guidance/information-security-guide-2013_WEB.pdf

12.2 How to comply

12.2.1 Take the following steps depending on how the information is held:

(a) Physical security:

- If personal information is contained in hard copy, keep it in locked filing cabinets in lockable rooms.
- Consider the installation of alarm and security systems.
- If personal information is in electronic form, keep it in a secure location with limited access based on a need-to-know basis.
- Ensure appropriate storage and movement of files are audited and monitored.

(b) Logical security:

- Install and use the latest technology firewalls, data encryption and anti-intrusion devices.
- Information and communications technology systems should be tested regularly.

(c) Access and use management:

- Have policies in place to restrict access, which should be administered by a dedicated staff member.
- Train workers in the privacy policies and procedures.

(d) Storage protocols:

- Have a classification for how documents should be stored, both onsite and offsite.
- Have procedures in place for removal of documents that are no longer to be retained.

(e) Internet and/or 'cloud' services providers:

- Ensure they have demonstrated a robust security system and provided the Church Body with appropriate undertakings, warranties and indemnities to protect and be responsible for the safe keeping of the data.
- Consider if they are located offshore and if so where.

12.3 Reasonable steps

What are 'reasonable steps' to secure personal information will depend on the Church Body's particular circumstances. The Security Guide indicates that some relevant factors could include:

(a) the nature of the entity holding the personal information;

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

(c) the risk to the individuals concerned if the personal information is not secure;

(d) the data handling practices of the entity holding the information; and

(e) the ease with which a Church Body can implement a security measure.

In determining 'reasonable steps', Church Bodies should give regard to these matters as well as those set out in 12.2 above.

12.4 How to comply:

12.4.1 Where there is a potential for unauthorised access to personal information, for example, health information (or any other personal and sensitive information) is displayed or distributed to staff members, take steps to ensure that unauthorised access to that information is minimised.

12.4.2 Remind staff members taking records of personal information offsite (e.g. on laptop computers) about the need to keep personal information secure, especially in the case of sensitive information where the adverse consequences of unauthorised access may be serious.

12.4.3 If electronic records of personal information are kept, take steps to ensure that personal information contained in databases is appropriately secure. This would include having restricted access, passwords that limit such access and other appropriate measures to prevent unauthorised access to records. Additionally, continue to ensure that appropriate firewalls and other security technology is applied to protect electronic records of personal information. This will also apply to the security of electronic communications that contain personal information.

12.4.4 Review the need for policies and security measures in respect of computer, electronic mail and Internet use.

12.4.5 Ensure appropriate warnings to ensure that workers do not divulge passwords, and the provision that electronic records are not accessed by unauthorised means are contained in computer or Internet use polices.

12.4.6 Implement comprehensive confidentiality and security procedures and provide training to all individuals who have access to personal information (such as employees, contractors, volunteers and clergy) as to the appropriate manner in which they should treat personal information.

12.4.7 Regularly monitor and audit these procedures for compliance to ensure their effectiveness. If a data breach occurs, Church Bodies should take immediate steps to prevent a repetition of the circumstances giving rise to the breach.

12.5 Destruction and permanent de-identification (APP 11.2)

12.5.1 Requirement:
Where personal information is no longer required for an authorised purpose, a Church Body must take reasonable steps to destroy or permanently de-identify the personal information.

12.6 Comment

12.6.1 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.

12.7 How to comply:

12.7.1 A Church Body should have in place systems for securely destroying or de-identifying personal information that it no longer needs for an authorised purpose.

12.7.2 In determining whether information is no longer required under APP 11.2, 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 Church Body's operations.

12.7.3 Ordinarily, garbage disposal or recycling of intact documents are not secure means of destruction. Church Bodies should only use these methods for destroying 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.

12.7.4 Consider discussing with the Church Body's insurer and/or legal adviser what records should be kept and for how long.

12.7.5 Determine when personal information is 'no longer required'. As long as a policy to retain data can be reasonably justified, there will be no infringement of this APP. This is a risk assessment issue for the Church Body.

12.7.6 If there is a conversion of information collected from hard-copy records to electronic databases, 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. This may be inappropriate in some cases.

Example:
Some Church Bodies consider it appropriate to update incorrect information on a database but retain the original (and now inaccurate) information in the original form in which it initially collected the information. The keeping of original records in such circumstances may be appropriate where the original record is required to compare a change in an individual's medical condition, or where it is necessary to retain the original record to verify what information the Church Body provided originally. However, in other cases it may be more appropriate to discard information contained in a hard-copy form, which the Church Body has converted to electronic form, for example, a leave request form. However, this will depend on the situation and type of information contained in the form.

12.7.7 In cases where the Church Body considers it necessary to retain information that is old or superseded, take steps 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.

12.7.8 Further, in the case of both electronic and hard copy records, ensure that procedures are in place whereby records that are no longer required are de-identified or destroyed. The destruction of information must be done by secure means (e.g. securely locked bins, shredding, pulping) and not by general disposal. A fixed annual review of personal information would be a way to ensure that a Church Body complies with this obligation.

12.8 Do's and Don'ts

DO consider how, and in what form, you store personal information, and consider how secure this is.

DO ensure that all hard copy records of personal information are kept securely locked or supervised.

DO locate personal information that is no longer needed. In such cases, the information should be destroyed or de-identified.

DO ensure that staff maintain adequate security of all personal information under their control.

DO limit access to personal information only to those who require it to carry out their duties for a permitted purpose (i.e. a 'need to know' basis).

DO contact the Church Body's privacy officer (the person in the Church Body that is responsible for privacy matters and compliance) if you are unsure as to the Church Body's practices and procedures for keeping personal information secure.

DO make a note of to whom personal information has been disclosed, for example, a record of who has a particular file, or who has access to a particular database.

DO scrutinise requests for disclosure of personal information, for example follow the

Church Body's procedure to identify an individual who asks you to disclose or 'check' their personal information.

DO ensure that in cases of shared computers, tools are implemented to avoid possible privacy breaches.

DO ensure that workers log in and out in accordance with allocated levels of access.

DO establish procedures for the destruction or de-identification of personal information that is no longer required.

DO consider the following matters when engaging a cloud service provider:

- the sensitivity of the data from a privacy perspective;
- the sensitivity of the data from a business operational perspective;
- in what jurisdictions may the data be stored by the cloud provider;
- is the data encrypted when transferred and stored; and
- what other forms of security does the provider use.

DO ensure the cloud service provider is subject to strict contractual provisions regarding security of the data and liability for any breach.

DON'T access, discuss, display, or disclose personal information other than as permitted by the APPs.

DON'T leave personal information unattended and not especially secure. For example, workers should shut down, log off or use a screensaver with a password when they leave their computers for an extended period. Do not leave files where unauthorised people may access them.

DON'T ever allow unauthorised access, modification or disclosure of personal information.

13. ACCESS (APP 12)

13.1 Access to Personal Information

13.1.1 Requirement

On request, a Church Body must provide the individual with access to his or her own personal information.

13.1.2 Exceptions to requirements

There are however some exceptions, which are:

(a) the Church Body 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 Church Body 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 Church Body 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 Church Body in connection with commercially sensitive decision-making processes (APP 12.3(j)).

13.1.3 Requirement

The Church Body 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 Church Body must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the Church Body and the individual (APP 12.5).

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

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

13.1.7 Where access is denied, the Church Body 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).

13.2 Comment

13.2.1 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.

13.2.2 *Unreasonable impact on the privacy of others*

Access to a document containing personal information about people other than the individual requesting access need not be denied altogether. For example, in such a case, it may be possible to delete or redact the other individual's personal information from the document before it is released to the individual who made the request.

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.

13.2.3 *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.

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

Providing access to personal information would be considered 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 (including a duty of care). Section 16 discusses the duties of common law. If a law requires a Church Body to refuse access, it must refuse access. If a law authorises a Church Body to refuse access, it means it may decide whether to provide or refuse access.

13.3 How to comply:

13.3.1 Establish a standard procedure whereby individuals are permitted to access their records except where an exception to the access principle applies. The Church Body is entitled to make a charge for providing access on a cost recovery basis.

13.3.2 Prior to collecting any personal information, ensure that the Church Body has systems in place to respond to access requests within a reasonable period and determine whether it should grant access. Individuals may request access through the Church Body's privacy officer (the person within the Church Body who is responsible for privacy matters and compliance) or delegate. The Church Body should also implement practices, systems and procedures to enable the Church Body to deal with inquiries and complaints about its compliance with the access provisions.

13.3.3 Although individuals are not required to give a reason to access their records, ask the individual what information or the type of information he or she wants to access. This is likely to help facilitate the individual accessing the information he or she is seeking.

13.3.4 APP 12 only gives individuals the right to access personal information that the Church Body holds about that individual. A Church Body should take adequate steps to verify the identity of the individual requesting access. This may include verifying that the Church Body has given an individual authority to access personal information on behalf of another individual. Such steps are likely to vary on a case-by-case basis. However, the Church Body should adopt the view that, in most cases, parents may have access to records relating to their child unless special circumstances arise.

13.3.5 The Church Body may refuse or restrict access to the record where an exception applies. One example might be where providing access would have an unreasonable impact on the privacy of others (APP 12.3(b)). Another example is the Church Body has reason to suspect that unlawful activity, or misconduct that relates to the Church Body's functions or activities has been engaged in and providing access would prejudice the taking of appropriate action by the Church Body (APP 12.3(h)).

13.3.6 APP 12 requires that organisations 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.

13.3.7 Where access is denied, take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the Church Body 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.

13.4 Do's and Don'ts

DO allow individuals to have access to, and copies of, their personal information, except where there are reasons to refuse access.

DO verify the identity of any individual seeking access to personal information.

DO respond to the request for access within a reasonable period.

DO inform people of their right to access their information, at the time of collecting personal information.

DO consider the following matters when an access request is made:

- what information the individual wants access to;
- whether the Church Body is permitted to refuse or restrict access;
- that there are various forms of access, including allowing the individual to inspect or take notes of the information, providing photocopies of the information, and giving the individual an accurate summary of the information;
- whether access can be given through the use of a mutually agreed intermediary;
- whether to charge the individual for access. Any charge must not be excessive.

DON'T provide an individual with direct access to information if that access would unreasonably affect the privacy of others or reveal a commercially sensitive decision-making process. Instead, **DO** consider whether the Church Body can provide an alternative form of access.

DON'T refuse an individual access to their personal information just because it may be costly, inconvenient or difficult to provide.

14. CORRECTION

14.1 Correction of Personal Information (APP 13)

14.1.1 If a Church Body holds personal information and either

(a) the Church Body 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 Church Body 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 Church Body corrects personal information about an individual that the Church Body previously disclosed to another entity, and the individual requests that other entity be notified of the correction, then the Church Body 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 The Church Body, upon denying a correction, 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 Church Body refuses to correct the information and the individual requests the Church Body to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, then the Church Body 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 Church Body 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).

14.2 Comment

14.2.1 *General obligation*

The principle is not intended to create a broad obligation on entities to maintain the accuracy 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 Church Body 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.

14.2.2 *'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 Church Body 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 the individual requests that notification. However, notification is not required if it would be impracticable or unlawful.

14.2.3 *Statement relating to information*

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

14.2.4 *Time periods*

A Church Body 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 thirty (30) days.

14.3 How to comply:

14.3.1 Establish a standard procedure where, at the time of use or disclosure of information, the Church Body assesses 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.

14.3.2 Consider what steps are reasonable in the circumstances to correct information where the individual requests it to be corrected, to ensure that information is accurate, up-to-date, complete, relevant and not misleading.

14.3.3 However, if there is a disagreement as to whether an individual's information is accurate, complete, up-to-date, relevant and not misleading, and if the individual requests it, take such steps as are reasonable in the circumstances to associate a statement about the individual's claim with the information.

14.3.4 Implement practices, systems and procedures to enable the Church Body to deal with inquiries and complaints about its compliance with the correction provisions.

14.4 Do's and Don'ts

DO assess the information you use and disclose, and correct it if necessary to ensure it is accurate, up-to-date, complete, relevant and not misleading.

DO consider what steps are reasonable in the circumstances to correct information upon request by the individual.

DO encourage individuals to notify the Church Body if they consider the personal information held about them is inaccurate, out-of-date, incomplete, irrelevant or misleading.

DO inform people of their right to correct their information at the time of collecting personal information.

DON'T refuse to correct personal information just because it might be costly, inconvenient or difficult to do so.

PART 3 SPECIAL ISSUES FOR THE CHURCH

15. CAPACITY TO CONSENT

15.1 Capacity

15.1.1 In order to give consent, the individual must have the capacity to give that consent. For an individual to have the capacity to consent, they must be capable of:

(a) understanding the nature of the decision they are making, including what the effect of giving or withholding consent would be;

(b) forming a view based on reasoned judgment; and

(c) communicating their decision.

15.1.2 In the APP Guidelines, it is recognised that an individual's capacity to consent may be affected by:

(a) their age;

(b) a physical or mental disability;

(c) a temporary incapacity, such as during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe stress, or suffering dementia; or

(d) a limited understanding of English.

15.1.3 The APP Guidelines state that an APP entity can ordinarily presume that an individual has the capacity to consent, unless there is something to alert it otherwise (e.g. the individual is a child).

15.1.4 Where the Church Body identifies an issue that may affect the individual's capacity to consent, it should consider whether the issue could be addressed by providing the individual with appropriate support, such as an interpreter or using an alternative method to communicate with the individual. If the individual still does not have the capacity to consent and consent is required, the Church Body should consider who could give consent on the individual's behalf. This could be:

(a) the individual’s legal guardian;

(b) someone with an enduring power of attorney;

(c) a person recognised by other relevant laws, for example in New South Wales, a 'person responsible' under the *Guardianship Act 1987* (NSW);

(d) a person whom the individual has nominated in writing while they were capable of giving consent.

15.1.5 The APP Guidelines recommend that even where an individual lacks capacity to consent, they should be involved in the decision-making process, and to the extent practicable have privacy issues communicated to them in a way that is understandable and comprehensible.

15.2 Consent and Young People

15.2.1 The Privacy Act does not distinguish between adults and children and thus clearly envisages that young people are to be afforded rights in respect of their privacy. However, the APPs do not differentiate between children of different ages and thus it is difficult to determine when it is appropriate to seek consent from young people.

15.2.2 The APP Guidelines provide as follows:

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

15.2.3 The Australian Law Reform Commission (**ALRC**) also considered the issue of consent by children and young people and recommended that the Privacy Act should be amended to provide that where an assessment of capacity to provide consent 'is not reasonable or practicable' an individual of the age of 15 or over should be capable of giving consent and a person under that age should be presumed not to be capable of giving consent.

15.2.4 The ALRC also noted that people with parental responsibility had some authority to make decisions on behalf of their children who lacked capacity if it was part of a duty to provide for their welfare but did not suggest that such authority extended to all situations. It should also be noted that a parent is recognised by the common law as having the right to make decisions concerning the child's education and to bring up their child in the religion of their choice. In all States and Territories, the age of majority is eighteen years.

16. DUTY OF CARE AND OBLIGATIONS OF CONFIDENCE

16.1 Duty of Care, Obligations of Confidence and the APPs

16.1.1 As discussed in Section 6, a Church Body generally can only collect sensitive information (including health information) with consent and can only use and disclose personal information for the purpose for which it was collected or a directly related secondary purpose. There are two important relevant exceptions to those general rules:

(a) where the person consents; and

(b) where required or authorised under a law.

16.1.2 In this context, 'law' includes the common law. The common law imposes a duty of care on Church Bodies, which they must exercise in relation to young, vulnerable or elderly people in their care. It can be contended that Church Bodies are required by this common law (duty of care), to collect certain personal and sensitive information in order to comply with this duty. This would justify the Church Body collecting sensitive information about such persons and possibly others (e.g. parents, contractors etc.) under APP 3.2 in order to fulfil its duty of care in its responsibility as the carer. A duty of care may also permit use and disclosure under APP 6 in circumstances where such disclosure would not be reasonably expected.

> Example:
> An example of where a duty of care may require disclosure would be a Church Body informing a third party temporarily in charge of a resident of an aged care facility that the resident suffers from a particular health problem.

16.1.3 The common law, in some situations, imposes upon people an obligation of confidence. In broad terms, confidence can be claimed where:

(a) the information is by its nature confidential;

(b) the information is communicated in circumstances importing an obligation of confidence; and

(c) disclosure of the information would be unauthorised by the provider or by law.

16.1.4 If personal information is given in confidence, it is clear that the provider would not wish it to be used by the Church Body or disclosed by the Church Body for purposes other than the purpose for which it was given. However, there may be occasions where such confidence can be breached if this is required in order for the Church Body to fulfil its duty of care. That said, it would be useful for Church Bodies to make it clear in, for example, a collection notice or Privacy Policy that there may be occasions where confidences cannot be maintained.

16.1.5 Another issue to keep in mind is that personal information provided by another person in confidence may still need to be disclosed if the subject of that information requested it from the Church Body under APP 12, as such disclosure may be authorised under law.

16.1.6 The uncertainty in this area only serves to underline the fact that records of confidential information should only be made where there is a need to do so and in the knowledge that access to the record may be sought.

16.1.7 A common law duty of care and obligation of confidence might be used to restrict an individual's access to records of personal information held about them in some cases.

17. PERSONAL INFORMATION AND THE CHURCH COMMUNITY

17.1 Passing Information in the Church Community

17.1.1 Church Bodies like to see themselves as 'communities'. The Church Body community will typically consist of clergy, religious, employees, contractors, volunteers and members of the congregation. As in any community, information about others is passed through the community and on occasions will be recorded. Thus, a note in a newsletter asking the community to pray for a sick parishioner may involve a 'technical breach' of the APPs if it involved disclosure of sensitive information, provided it was contained in a record, but is unlikely to cause offence. However, on occasions it may, particularly if the individual wished their illness to be confidential, therefore caution should be exercised in this regard.

17.1.2 As the practices of Church Bodies may be well known in the community, consent to collection may well be implied in many circumstances because by providing their information as part of that community individuals will reasonably expect that their information will be disclosed in the community for a purpose that is related (or directly related) to the purpose for which their information was originally obtained.

17.1.3 The guiding principle in such cases is to show sensitivity in exercising a judgement as to when it is appropriate to disclose this type of information.

17.2 Religious Information

17.2.1 Where a priest or another Church Body seeks religious information about an individual, it would be wise to obtain consent. Church Bodies can achieve this in appropriate applications or other forms.

17.3 Fundraising

17.3.1 Disclosure of information for fundraising purposes raises greater difficulty. However, it is suggested that Church Bodies usually rely on extra funds raised via approaches to members of the congregation and that this would be a reasonably expected related secondary purpose. However, to ensure that it is expected it would be wise to include that fact in a collection notice.

17.4 Passing personal information to other Church Bodies

17.4.1 Where another Church Body requests personal information about an individual, in usual circumstances this information should not be passed on without consent. It may be done on occasions as part of the Church Body's duty of care or where the Church Body is required or authorised by another law to disclose the information to the other Church Body.

17.4.2 Church Bodies, which are related entities, may share personal information other than sensitive information, subject to restrictions on its use. See Paragraph 2.6.8 as to when Church Bodies may be considered related entities.

17.5 Church Body Publications

17.5.1 Church Body publications, such as newsletters and magazines, often contain personal information obtained either from the relevant individual or from other sources. These publications could be said to be 'generally available publications', even if the Church

Body only distributes these publications within the Church Body community, provided they could be made available to the public on request. It is also arguable that a Church Body website available to the public is a generally available publication. The effect of this is that although the information may be a 'record' when collected, it can be freely used and disclosed through dissemination of the publication.

17.5.2 Ideally, personal information, which a Church Body collects for inclusion in a publication, should be collected directly from the individual, particularly where the information relates to a personal or private matter. Where this is impracticable, the APPs require that the individual be made aware of the matters required under APP 5.2 (see Section 6). A Church Body would generally achieve this by sending the individual a copy of the publication.

18. HEALTH INFORMATION

18.1 Protection of Health Information

18.1.1 Health information enjoys special protection under the Privacy Act and under the following State and Territory legislation:

(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).

18.1.2 Some Church Bodies collect substantial amounts of health information about, for example, residents of aged care facilities operated by the Church Body. They need to take particular care in collecting, using and disclosing health information.

18.2 What is Health Information?

18.2.1 Under the Privacy Act '*health information*' includes information or an opinion about:

(a) the health or disability of an individual; and

(b) a health service to be provided to the individual.

18.2.2 The Privacy Act provides that a '*health service*' includes an activity performed to assess, record, maintain or improve an individual's health, to diagnose an illness or disability, or to treat an individual. Legislation in some States and Territories specifically includes '*mental and psychological*' health as being health information. Church Bodies should treat health information as including information about an individual's mental and psychological health. Therefore, a report from a Church Body counsellor or a consultant psychologist will often contain health information.

18.2.3 Accordingly, a Church Body may trigger the health information provisions in circumstances including where it engages:

(a) a nurse;

(b) a counsellor;

(c) a psychologist; or

(d) a sports physiotherapist,

who assesses, records, maintains or improves an individual's health, diagnoses an individual's illness or disability, or treats an individual. The provisions are not intended to apply where, for example, a member of staff carries out emergency first aid on an individual.

18.2.4 If a Church Body is unsure as to whether it is providing a 'health service', it should treat the health information with the higher level of protection afforded by the health information provisions. These are discussed below.

18.3 Collection of Health Information

18.3.1 Health information generally should only be collected:

(a) with the consent of the individual or their guardian;

(b) where it is required to allow the Church Body to exercise its duty of care or is otherwise required or authorised by law; or

(c) where it is necessary to lessen or prevent a serious threat to the life, health or safety of an individual and it is impracticable to obtain consent.

18.3.2 In most cases in Church Bodies, the collection will be with the consent of the individual or, where the individual lacks capacity, the consent of the guardian or other responsible person. In some cases, however a Church Body may collect information from a third party, such as an independent doctor attending an aged care facility to treat a resident, in circumstances where it is necessary for the Church Body to exercise its duty of care.

18.3.3 Where a Church Body itself records incidents at Church Body where an individual suffers an injury, this will constitute collection of health information. This is required if the Church Body is to exercise its duty of care.

18.4 Use or Disclosure of Health Information

18.4.1 It is important to remember that health information, in particular, usually should only be used or disclosed:

(a) for the purpose for which it was collected or a **directly** related secondary purpose;

(b) to exercise the Church Body's duty of care or as otherwise required or authorised by law; or

(c) to lessen or prevent a serious threat to the life, health or safety of an individual and where it is impracticable to obtain consent.

18.4.2 A Church Body should not disclose health information of an individual to third parties unless it considers that it is reasonably necessary to disclose it to ensure that it maintains the health or safety of the individual.

18.4.3 In order to provide appropriate protection to health information it is also important that it be kept secure and only staff who have a need to know the information are given access to it.

18.4.4 If it is necessary to include the information in a notice to staff, care should be taken that the notice is not accessible by non-staff members.

18.5 Health Information and Employees

18.5.1 As discussed at Section 19, certain acts or practices directly relating to employee records are exempt from the scope of the Privacy Act. An employee record relates to the employment of an employee of the employer. Health information of an employee may sometimes be considered as part of an employee record where it directly relates to a current or former employment relationship between the employer and the individual.

18.5.2 In New South Wales, the Health Records and Information Privacy Act 2002 (NSW) will not cover information about an individual (including health information) that forms part of an employee record within the meaning under the Privacy Act. The same exemption is not contained within the *Health Records Act* 2001 (Vic) and *Health Records (Privacy and Access) Act* 1997 (ACT). In those jurisdictions, health information, which is contained in an employee record, will be covered by the provisions of that legislation.

18.6 Additional Requirements in States and Territories

18.6.1 In New South Wales, the *Health Records and Information Privacy Act* 2002 (NSW) implements a privacy regime for health information held in the New South Wales public sector and the private sector (except small businesses as defined in the Privacy Act). The Act allows individuals to obtain access to health information and establishes a framework

for the resolution of complaints regarding the handling of health information. The Act contains 15 Health Privacy Principles that outline how health information must be collected, stored, used and disclosed. The Act applies to persons who have been deceased for a period of 30 years or less.

18.6.2 In Victoria, the *Health Records Act* 2001 (Vic) covers the handling of all health information held by health service providers in the state public sector and the private health sector. The Act contains 11 Health Privacy Principles adapted from the NPPs. The Act applies to persons who have been deceased for a period of 30 years or less, as well as small business operators. As noted above, the Act also applies to information contained in employee records.

18.6.3 In the ACT, the *Health Records (Privacy and Access) Act 1997* (ACT) regulates the handling of health records held in the public sector in the Australian Capital Territory and also applies to acts or practices of the private sector. The Act contains 14 Privacy Principles that have been modified to suit the requirements of health records. The Act applies to deceased persons in the same way as they apply in relation to an individual who is not deceased. As noted above, the Act also applies to information contained in employee records.

18.6.4 *Dealing with children*

There are also specific provisions regarding the rights and powers of young people under the various State Acts. They are summarised below.

New South Wales	A child may not rely on any right or powers conferred under the *Health Records and Information Privacy Act* 2002 (NSW) if the child is incapable (despite the provision of reasonable assistance by another person) by reason of age of understanding the general nature and effect of, or communicating their intentions, with respect to that particular provision. In such cases, an authorised representative of a child, such a parent or guardian, may act on their behalf.
Victoria	The *Health Records Act* 2001 (Vic) provides that a complaint about a breach may be made by a child or on behalf of the child by a parent, any other person chosen by the child, or any other person who the Health Services Commissioner determines has a sufficient interest in the subject matter of the complainant. Additionally, a child may request access to or correction of health information only where they are capable of understanding the nature and effect or making such a request or communicating the request personally. Otherwise, an authorised representative (such as a parent or guardian) of the child may exercise the right to make that request.
ACT	The *Health Records (Privacy and Access) Act 1997* (ACT) provides that a right or power conferred upon a young person (being a person under 18 years of age, other than a person who is of sufficient age and mental and emotional maturity to understand the nature of and give consent to a health service) by the Act is exercisable only by a guardian of the young person, and is not exercisable by a young person on their own behalf.

18.7 Inconsistencies between Federal and State laws

18.7.1 In addition to the Privacy Act, Church Bodies in New South Wales, Victoria and the Australian Capital Territory who are recognised as providing a health service will also be required to comply with the relevant health information legislation in those jurisdictions. Such Church Bodies will therefore be required to comply with two sets of principles: the APPs in the Privacy Act and the relevant set of Health Privacy Principles or Privacy Principles, which in some cases will impose different standards.

18.7.2 The scope of the State and Territory legislation may also differ from the federal legislation. For example, the Victorian Act covers small business operators and employee records, unlike the Privacy Act. The information handling principles in the New South Wales, Victorian and Australian Capital Territory legislation also differ from each other, so that information passing from one jurisdiction to the other may become subject to a different set of rules. This is something Church Bodies should bear in mind if they are transferring such information to other jurisdictions.

18.7.3 The Privacy Act expressly allows State and Territory privacy legislation to operate to the extent that such laws are not directly inconsistent with the Privacy Act. Insofar as the various Health Privacy Acts provide more stringent provisions than the Privacy Act but do not contradict it, Church Bodies are required to comply with both sets of legislation.

19. EMPLOYEE RECORDS

19.1 Employee Records

19.1.1 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 organisation relating to the individual.

19.1.2 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, remuneration, termination and trade union membership.

19.1.3 The employee records exemption does not extend to prospective employees, contractors, consultants or volunteers. In New South Wales the health records of an employee will not be considered ‘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. If this applies to your Church Body, see Section 18.

19.1.4 The exemption will only apply to an employee record held by the employing organisation. Once the record is disclosed to another entity, the exemption will cease to apply and the APPs will govern the handling of that information in the hands of the new entity holding the record. This is of particular importance where a Church Body has access to employee records (for example via a database, or centralised HR facility) of employees of another Church Body. In such cases, the Church Body, which is not the employer of the individual to whom the records relate, will be subject to the requirements of the Privacy Act in collecting, using and disclosing those employee records. It also means that where a Church Body holds employment information for the employees of other Church Bodies (e.g. priests), those employees *will* be able to access (under APP 12) their personal information because their employer does not collect it.

19.1.5 Acts of employers who use employee information for commercial purposes outside the employment context will not be exempt from the operation of the Privacy Act. Under the Privacy Act, examples of employee records include health information about an employee and personal information about any or all of the following:

(a) the engagement, training, disciplining or resignation of the employee;

(b) the termination of the employment of the employee;

(c) the terms and conditions of employment of the employee;

(d) the employee's personal and emergency contact details;

(e) the employee's performance or conduct;

(f) the employee's hours of employment;

(g) the employee's salary or wages;

(h) the employee's membership of a professional or trade association;

(i) the employee's trade union membership;

(j) the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and

(k) the employee's taxation, banking or superannuation affairs.

19.1.6 Some practices in relation to employees could possibly fall outside the employee records exemption. For example, a record of a staff member's place of birth (collected via a 'Banking Information Form') might not be directly related to the employment relationship and therefore not within the 'employee records' exemption.

19.1.7 Whether or not information of this nature will be considered as being 'directly related' to the employment relationship will be a question of fact to be decided in the context of each case. However, the Church Body should bear in mind the consequences of having information that falls outside the employee records exemption.

19.1.8 Where a record of employee personal information falls outside the employee records exemption and is subject to the Privacy Act, then it is only that part of the record that falls outside the exemption that will be subject to the Privacy Act and not the whole record.

19.1.9 If employee records are given to related organisations, no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

19.2 Recommendation

19.2.1 If employee records are disclosed to a third party (including another Church Body), the Church Body should be aware that it will not be an 'employee record' in the hands of that third party and a collection notice may need to be given by or on behalf of the third party.

19.2.2 If employee records are given to related organisations no collection notice need be given, but the employee exemption will not apply in the hands of that related organisation.

19.2.3 Where employee records are given to third parties to enable them to provide advice, an issue of access may arise. Consideration would need to be given to whether there are grounds for resisting access.

ANNEXURE 1 – TEMPLATE PRIVACY POLICY

1.1 Overview

1.1.1 A Privacy Policy is needed to inform individuals about the practices of the Church Body in relation to personal information. It also serves as a guide to the Church Body's staff as to the standards to be applied in respect of handling personal information and ensure consistency in the Church Body's approach to privacy.

1.1.2 The following template Privacy Policy is intended to assist the Church Body to develop a Privacy Policy that satisfies the requirements of APP 1.4, dealing with openness.

1.1.3 The Privacy Policy which the Church Body adopts may be used, in conjunction with the collection notices, to satisfy the requirements in APP 5.2 to ensure that individuals are aware of relevant matters on collection of personal information.

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

Template Privacy Policy

This is a template privacy policy, which Church Bodies may adapt as appropriate to reflect the Church Body's particular acts and practices. The ***drafting notes*** *have been included to assist Church Bodies to adapt the document to their circumstances and provide examples of what sorts of details should be included.*

Privacy Policy

Your privacy is important to us

[***Clearly identify the Church Body***] complies with the *Privacy Act 1988 (Cth)* (**Privacy Act**) and the Australian Privacy Principles (**APPs**) in the Privacy Act. We respect and value the personal information that you are willing to entrust to us, and this policy explains how we collect, hold, use, disclose and otherwise manage that personal information. [***Remove the following if no school (or other body) attached to Parish***] It does not relate to records collected and held by the Parish school. The school has a separate policy statement, which is available on request from [***insert name and contact number***] or on their website.

We may from time to time review and update this policy to comply with our legal obligations, to reflect changes in technology and to our operations and practices, and to ensure it remains relevant to our environment. [***Insert how changes to the policy will be effected– e.g. published on website, in newsletter, etc.***]

What kind of personal information do we collect and how do we collect it?

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the information or opinion is true or not, or whether it is recorded in a material form or not.

Sensitive information is a subset of personal information, which is given a higher level of protection under the Privacy Act. It includes, amongst other things, health information about you, your criminal record and your religious beliefs or affiliations.

We collect and hold personal information, which may include sensitive information about:

[***The following list should be adapted so that is relevant to the particular Church Body. All types of personal information that the Church Body regularly collects should be included. The list below is an example of what a Parish might say.***]

- children and their parents and/or guardians and may be related to children receiving sacraments or pastoral care. It may relate to the child's enrolment at the Parish school, after school care facility or sporting association;
- adults receiving sacraments or pastoral care and witnesses to sacraments;
- job applicants, volunteers and contractors; or
- fundraising, including banking or other payment details.

Personal information you provide.
We will generally collect your personal information by way of [***insert relevant examples, such as the following***] forms filled out either by the individual or their guardian/responsible person, face-to-face meetings, interviews and telephone calls.

Personal information provided by other people.
In some circumstances, a third party including other parishes, may provide us with your personal information, e.g. a reference about an applicant for a position, [***insert other examples as appropriate***].

In some cases where you do not provide personal information we request, [***insert consequences of failure to provide information – for a Parish this might be as follows***] you or your child may not be able to receive the sacrament or be enrolled in the Parish program, or the Parish may not be able to assess your job or volunteer application.

You may also choose to deal with us on an anonymous basis or using a pseudonym. However, we will need to identify you in many circumstances, for example, to administer certain sacraments or to provide, care for your children or to process a job or volunteer application. [***Where the Church Body is operating an aged care facility, it may not be possible for individuals to deal with it on an anonymous or pseudonymous basis. If that is the case state here.***]

How will we use the personal information you provide?

We will use personal information we collect from you to:

[***The following list should be adapted so that is relevant to the particular Church Body. All regular uses of personal information by the Church Body should be included. The list below is an example of what a Parish might say.***]

- administer the sacraments and pastoral care;
- keep you informed about matters relating to spiritual life, through correspondence and newsletters;
- look after your spiritual and physical wellbeing;
- provide care for your child(ren) while under our supervision;
- fundraise, seek and administer donations;
- tell you about events and developments in the Church and our community;
- assess your job or volunteer application;
- manage our volunteers;
- satisfy the Parish's legal obligations and allow the Parish to discharge its duty of care.

To whom might we disclose personal information?

In particular circumstances, we may, disclose personal information held about an individual to:

[***The following list should be adapted so that is relevant to the particular Church Body. All regular disclosures of personal information by the Church Body should be included. The list below is an example of what a Parish might say.***]

- another Parish or the Diocese/Archdiocese of [***insert***];
- government departments;
- medical practitioners;
- people providing services to the Parish, including volunteers and any third party service providers;
- recipients of Parish publications;
- parents and/or guardians;

- if required or authorised by an Australian law or court/tribunal order
- anyone to whom you authorise the Parish to disclose information.

Overseas disclosures: We will only disclose personal information about you or your child outside Australia where you have requested that we do so. Where you make such a request, you agree and acknowledge that we will have no control over the information that we disclose, and that we will not be able to ensure that the overseas recipient handles that information in accordance with the Privacy Act, the Australian Privacy Principles and any other applicable Australian laws.
[***If the Church Body is likely to disclose personal information to overseas recipients in circumstances other than when requested by the individual, this will need to be stated here as well as the countries that those overseas recipients are likely to be located in (if practicable to specify).***]

Direct marketing

You may opt out of receiving communications from us about our services and activities including fundraising, at any time by contacting us on the details below.

Management and security of personal information

Our workers are required to respect the confidentiality of the information and privacy of individuals. We have in place steps to protect the personal information we hold from misuse, interference, loss, unauthorised access, modification or disclosure by use of various methods including locked storage of paper records and password restricted access rights to computerised records.

Where we no longer require personal information for a purpose for which we can use or disclose it under the Privacy Act, we will take reasonable steps to destroy or de-identify that information, unless it would be unlawful for us to do so.

Correction and updating personal information

We endeavour to ensure that the personal information we hold is accurate, complete, and up to date, and where using or disclosing it, relevant for the purpose of the use or disclosure.

A person may seek to update the personal information we hold about them by contacting us at any time on the details below. If we are unable to correct your information, we will give you notice of this in writing and explain why and how you can take the matter further. You can also request that we associate a statement with the information that you believe is inaccurate, out-of-date, incomplete, irrelevant or misleading.

Access to personal information we hold about you

You may access any personal information that we hold about you. Parents or guardians can generally make such a request on behalf of their children. To make a request for access, please put your request in writing and send it to us on the details below.

We may require you to verify your identity and specify what information you require before we can provide access. In some circumstances as provided for by APP 12, we may be unable to

provide access, in which case we will notify you of this in writing and explain why and how you can take the matter further.

We will not charge you for making a request; however, we may charge you our reasonable costs of providing access to any information requested.

Consent and right of access to the personal information of children
[***If the Church Body does not regularly deal with children, for example if its function is to operate aged care facilities, then it may be appropriate to remove this section or to amend it to deal more generally with issues of capacity.***]

We assess whether a child has the capacity to make their own privacy decisions on a case-by-case basis, having regard to matters such as their age and circumstances. Generally, individuals over 15 years will have the capacity to make their own privacy decisions.

For children under 15 years or who otherwise do not have capacity to make these decisions for themselves, we will refer any requests for consent and notices in relation to personal information to the parent and/or guardian. We will treat consent given by a parent and/or guardian as consent given on behalf of the child and notices to parent and/or guardians will act as notice given to the child.

Enquiries and complaints

If you would like further information about the way we manage personal information, please contact us on the details below.

Contact details

[*Insert Church Body's contact details including a contact person, the address, telephone and email (where possible)*]

If you believe that we have acted contrary to this Policy or the Privacy Act, please put your complaint in writing and send it to us using the details above. We will investigate your complaint and try to resolve it. However if you are not satisfied with the response, you can contact the Office of the Australian Information Commissioner (OAIC) on 1300 363 992 to make a query about your privacy rights, or visit www.oaic.gov.au for more information about how to lodge a complaint. The OAIC has the power to investigate the matter and make a determination.

This Privacy Policy was last updated [*insert date*]

ANNEXURE 2 – TEMPLATE COLLECTION STATEMENTS

A collection statement is needed to inform individuals about the collection of their personal information and how the Church Body will handle that personal information.

Collection statements will vary significantly because the information they contain will depend on the type of information being collected, how it is being collected, the purpose of collecting the information, and to whom the information might be disclosed.

The collection statement checklist below is designed to assist Church Bodies to draft collection statements that meet the requirements of APP 5.

Collection statement checklist

Every collection statement that a Church Body prepares should cover the following matters .

	Requirement	**Example drafting**
☐	Identity of the Church Body and contact details (unless obvious or can easily be located)	*The Archdiocese of ## collects the personal information contained in this form in order to* [insert purpose of collection]
☐	If the information has been/will be collected from a third party or the individual is otherwise not aware of the collection, then the fact that the collection has taken place and the circumstances of that collection.	*We will also collect your personal information, including sensitive information, from other health service providers who treat you.*
☐	The purposes for which the Church Body collects the information	*We collect your personal information, including sensitive information, in order to* [insert the purpose of collection]
☐	If the collection is required or authorised by or under and Australian law or court/tribunal order – then the fact that it is so required or authorised including the name of the law or details of the order	*We need to collect this information in order to discharge our duty of care.* OR *We are required to collect this information under*
☐	The main consequences if the Church Body does not collect the information	*If you do not provide this information then we may not be able to* [insert main consequences, e.g. provide services, administer a sacrament, etc.].
☐	Any other purposes for which Church Body is likely to use or disclose the information (while this is not included in APP 5.2 matters, it will help to create a 'reasonable expectation' of potential secondary uses and is also part of meeting the Church Body's obligation to be	*We may also use the information you provide to contact you about other services we offer and about our fundraising efforts.*

	open and transparent)	
☐	The other entities or types of entities to which the Church Body usually disclosed personal information of the kind being collected	*We may disclose your personal information to third parties such as our contracted service providers, some of which are located overseas, including in New Zealand and the USA.*
☐	Whether the Church Body is likely to disclose the personal information to overseas recipients, and if so the countries in which such recipients are likely to be located (if practicable to specify)	
☐	That the Church Body's Privacy Policy contains information about how the individual may access personal information that the Church Body holds about them and seek correction of such information	*For more information about how we handle your personal information, including how to access and correct it, how to make a complaint and how we handle complaints, see our Privacy Policy available at* [insert where/how applicant can access the Privacy Policy e.g. via a website, by calling or emailing]
☐	That the Church Body's Privacy Policy contains information about how the individual may complain about a breach of the APPs (or any registered code which binds the Church Body), and how the Church Body will deal with such a complaint	

Template standard collection notice for Parish

The following is a template collection statement for a Parish. Other Church Bodies may use this as a guide in conjunction with the collection statement checklist above to develop their own standard collection statements.

1. [***Insert name of Church Body***] collects personal information, including sensitive information, to [***insert relevant purposes, e.g. enable the Parish to provide religious services to its community including administering the sacraments, and pastoral care to the faithful, including to children of the faithful***]. Information may need to be collected to allow us to meet our legal obligations, to provide care for children while under our supervision and to discharge our duty of care. If you reside in the Parish or otherwise use its services, the information may also be used to solicit donations and/or request and engage your services as a volunteer from time to time. As a member of the faithful or someone who wishes to become a member or participate in the Parish, you agree that the Parish will be collecting information about your religious affiliation or beliefs.

2. The Parish may need to disclose your personal information to third parties for administrative and fundraising [***insert any other***] purposes such as to other Parishes, the Archdiocese, medical practitioners and people providing services to schools, including volunteers. If you ask us to send your personal information overseas you agree that the Parish will have no control over the information disclosed and cannot ensure that the overseas recipient handles that information in accordance with the Privacy Act. [***NOTE: only inserted reference to overseas disclosure in this statement as it is the most applicable***] If we do not receive the information requested, we may not be able to provide our services, such as administering the sacraments or supervising and providing care to children.

3. Any consents that are required for the use and disclosure of the personal information collected about children will be sought from their parents or guardians unless the child is 15 years or more, in which case the Parish may seek the child's consent if it considers this appropriate in all the particular circumstances [***Note: consider if this reflects preferred approach especially if there is a parish school and the school has a particular policy – this statement is consistent with the APP Guidelines***].

4. For more information about how the Parish handles your personal information, how to access and correct it, how to make a complaint and how we handle complaints, see our privacy policy available at [***insert where/how applicant can access the Parish's privacy policy e.g. via the website, by calling or emailing***].

Template Job Application Collection Notice

The following is a template collection statement for Church Bodies when collecting personal information from a job applicant.

1. In applying for this position, you will be providing [***name of Church Body***] with personal including sensitive information. We can be contacted [***insert contact details***].

2. We will collect this information in order to assess your application and you agree that we may collect, use and disclose it for this purpose. If you do not provide or assist us in obtaining, the information requested, we might not be able to consider your application.

3. We may disclose your information to any referees whose information you have provided [***and insert types of organisations or particular organisation that the Church Body is likely to provide this information to – e.g. the relevant diocese and/or archdiocese, any third party service providers, etc.***].

4. [***If applicable insert the following***] We are required to conduct a criminal record check [***AND/OR***] collect information regarding whether you are or have been the subject of an AVO and certain criminal offences under Child Protection law before employment can be offered.

5. For more information about how we handle your personal information, how to access and correct it, how to make a complaint and how we handle complaints, see our privacy policy available at [***insert where/how applicant can access the Church Body's privacy policy, consistent with other collection statements and privacy policy***].

Template Contractor/Volunteer Collection Notice

The following is a template collection statement for Church Bodies when collecting personal information from an applicant contractor or volunteer.

1. In applying to provide your services, you will be providing [***name of Church Body***] with personal including sensitive information. We can be contacted [***insert contact details***].

2. We will collect this information in order to assess your application. If you do not provide the information requested, or assist us in obtaining the information, we may not be able to consider your application.

3. We may disclose your information to a third party, including any referees whose information you have provided [***and insert types of organisations you are likely to provide the information to – e.g. the relevant diocese and/or archdiocese***].

4. [***If applicable, insert following***] We are required to conduct a criminal record check [***AND/OR***] collect information regarding whether you are or have been the subject of an Apprehended Violence Order and certain criminal offences before a contract can be awarded [***OR***] before a position as a volunteer can be offered.

5. For more information about how we handle your personal information, how to access and correct it, how to make a complaint and how we handle complaints, see out privacy policy available at [***insert where/how applicant can access the Church Body's privacy policy, consistent with other collection statements and privacy policy***].