Privacy Policy and Information Sharing Policy

The Archdiocese of Canberra-Goulburn **(Archdiocese)** is committed to upholding the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth) **(Privacy Act)**. This Privacy Policy and Information Sharing Policy **(Policy)** sets out how the Archdiocese manages personal information and protect privacy.

This Policy is a document drafted to assist the employees within the Archdiocese in managing personal information as well as assisting the general public understand how personal information is collected, used and disclosed by and within the Archdiocese.

This Policy is intended to provide comprehensive but general guidance to staff of the Archdiocese (including Archdiocesan agencies) in relation to the collection, use and disclosure of personal information. Some organisations and agencies within the Archdiocese have their own privacy policies relating to specific circumstances under which personal information may be collected, used or disclosed. Staff of those organisations should read and comply with that organisation's privacy policy if they are dealing with personal information collected, used or disclosed by that organisation in those circumstances. Third parties dealing with such organisations should also be aware of the contents of those policies. For example, a teacher of a systemic school within the Archdiocese should comply with this Policy and the privacy policy of the Catholic Education Office if he or she is dealing with the personal information of a child from the school. Likewise, a parent of students attending a systemic school within the Archdiocese should be aware of the provisions of this Policy and the privacy policy of the Catholic Education Office in relation to how personal information of students and parents are handled by schools. Where there is no other relevant privacy policy, staff of the Archdiocese should comply with this Policy.

1.0 INTRODUCTION AND DEFINITIONS

1.1 Australian Privacy Principles

The Archdiocese is an "organisation" as defined in the Privacy Act and must comply with the requirements of the Privacy Act (as well as other related laws to be discussed below). One such requirement is the obligation to comply with the Australian Privacy Principles (**APPs**). The APPs set out the standards, rights and obligations in relation to the handling, holding, access and correcting personal information. There are 11 APPs which will be dealt with in turn in this Policy.

There are some instances where the Archdiocese may not be required to comply with the Privacy Act, for example, when handling employee records (see section 15.0 below for more information).

1.2 Personal information

The Privacy Act governs how "personal information" is to be handled. "Personal information" is a broad term defined in the Act, and generally means any information or opinion (whether true or not) about an individual that identifies the individual or from which that individual's identity reasonably can be determined.

A "person" is any individual, whether he or she is a member of the public, an employee of the Archdiocese, a priest, a child etc.

Examples of personal information include a person's:

- Name
- Signature
- Address
- Telephone number
- Date of birth
- Financial information
- Visual appearance (as captured in print or video)
- Employment details
- Commentary or opinion about a person

The above is a non-exhaustive list, and what constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the circumstances.

The definition of "personal information" is broad, and includes the following:

- Information not reduced to a material form (e.g. not written down or recorded), such as a verbal conversation between two or more people;
- information of one person can also be personal information of another person. For example, a marriage certificate will have personal information of both parties to the marriage; and
- combination of various pieces of information, for example, a common surname combined with an address could become personal information if that makes the person reasonably identifiable.

1.2.1 Persons dealing with personal information within the Archdiocese must be mindful of the above broad definition of personal information and treat such information in accordance with this Policy.

1.2.2 A kind of personal information is **"sensitive information"**. This term is also defined in the Act. The term includes the following kinds of information or opinion about a person:

- Racial or ethnical 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;
- Criminal record; and
- Health information about an individuals, including genetic information, biometric information and biometric templates.

Sensitive information is generally afforded a higher level of privacy protection under the Privacy Act compared to other personal information. Staff within the Archdiocese must be mindful of the distinction between sensitive information and other kinds of personal information when handling such information.

1.2.3 The handling of personal information is different where a **"permitted general situation"** exists. There are 5 such relevant situations:
a) Collecting, using or disclosing personal information to lessen or prevent a serious threat to life, health and safety (e.g. collecting or disclosing personal information of a parent to assist a child who may be at risk of abuse by a parent, on the basis it would be unreasonable to obtain the parent's consent).
b) Collecting, using or disclosing personal information as a means of taking appropriate action in relation to suspected unlawful activity or serious misconduct (e.g. if there are grounds to suspect misconduct from a professional advisor).
c) Collecting, using or disclosing personal information to locate a person reported missing;
d) If collecting, using or disclosing personal information is reasonably necessary for establishing, exercising or defending a legal or equitable claim; or
e) if collecting, using or disclosing personal information is reasonably necessary for a confidential alternative dispute resolution process.

2.0 APP1 – OPEN & TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

This principle requires the Archdiocese to manage personal information in an open and transparent way, including having a clearly expressed and up-to-date privacy policy.
This Policy has been drafted to comply with APP1. A summary of this Policy is available at http://cgcatholic.org.au/.

3.0 APP2 – ANONYMITY & PSEUDONYMITY

Individuals must have the option to deal anonymously or by a pseudonym with the Archdiocese, unless it is impracticable for the Archdiocese to do so or if the Archdiocese is required by law to deal with identified individuals.

Examples where individuals can deal with the Archdiocese anonymously or by using a pseudonym include where the individual is seeking general information (e.g. when a community event will take place) or contact information (e.g. the telephone number of a parish office)

3.1 When impracticable to deal with unidentified persons

If an individual does not wish to be identified, the Archdiocese might not be able to provide that individual with the information he or she has asked for or to give that individual the level of service he or she may expect.

Examples of where it would be impractical to deal with an individual who is not identified

include:

- If the individual wishes to make a complaint to the Archdiocese, it may be impractical for the Archdiocese to investigate or handle the complaint without knowing the complainant's information, such as his or her name; or
- if the Archdiocese is asked to provide information to someone, it would not be able to do so without knowing the name and contact details of the addressee.

3.2 When required or authorised by law

The Archdiocese does not have to deal with a person who does not want to be identified if the Archdiocese is required or authorised by law, or a court/tribunal order, to deal with individuals who have identified themselves.

The following examples of where a law or order may require or authorise the Archdiocese to deal only with identified individuals:

- Discussing the individuals' personal information with them, such as account information;
- giving access to personal information under the Privacy Act;
- opening a bank account for an individual; and
- providing assistance to a suspected victim of child abuse, whose injury is covered by a mandatory reporting requirement (see section 16 below).

4.0 APP3 – COLLECTION OF SOLICITED PESONAL INFORMATION

4.1 Why personal information needs to be collected

The Archdiocese may only collect personal information that is reasonably necessary for one or more of its functions or activities.

The Archdiocese carries out a multitude of functions, services and activities for the purposes of promoting the Catholic faith within the Archdiocese of Canberra-Goulburn. This includes, among other things, serving the Catholic Church community within the Archdiocese of Canberra-Goulburn, assisting and supporting parishes within the Archdiocese, liaising with members of the public, managing various ministries, such as hospitals, nursing homes and children's welfare centre and supporting the education office that manages the systemic schools within the Archdiocese.

The Archdiocese collects personal information from individuals when it is reasonably necessary to enable the Archdiocese to carry out its mission, activities and ministries or to assist individuals should they have an enquiry. The Archdiocese may also collect personal information for secondary purposes for which a person would reasonably expect the Archdiocese to use or disclose his or her personal information.

4.2 What kinds of personal information is collected

The type of information the Archdiocese may collect and hold varies depending on the purpose for which it is collected (see above). Depending on the circumstances, it could include one or more of the following:

- Name
- Address and other contact details, such as phone number, email address
- Date of birth
- Marital status

- Religious affiliation
- Health information
- Bank account details and financial information
- Employment history
- Government issued identification documents and numbers (e.g. driver's licences, tax file numbers)
- Photographs and videos of the individual

The above is a non-exhaustive list of kinds of personal information that could be collected.

Examples where one or more of the above may be required include:
- Information regarding religious affiliation and marital status is required to process a marriage application within a parish;
- health information is required to assess the suitability of admission into a retirement village or nursing home;
- bank account details are required if the Archdiocese needs to pay money to an individual;
- employment history information is required to consider employment of a person within the Archdiocese;
- photos and videos are required if the person has consented for their photo or video to be taken and used for news stories to be published in respect of Church related events and activities; and
- Working with Children Check or Vulnerable People registration details is required to be recorded for employees and volunteers working with children and other vulnerable persons.

It is important that only reasonably necessary personal information is collected for the relevant functions or activities of the Archdiocese are collected. For example, it would not be necessary to know a person's occupation in arranging a marriage ceremony, therefore such information should not be collected.

4.3 How personal information is collected

Generally speaking, personal information will be collected directly from an individual, for example, face-to-face, by phone or by email from the individual, or via a form submitted by the individual.

The exception to the above rule is if it would be unreasonable or impracticable to collect personal information only from the individual. For example, it would be acceptable to collect the personal information (e.g. names) of a number of people attending a Church event from one contact person, rather than having to contact each person individually for such information.

In most cases, consent from the individual specific to any collection is required. The consent may be explicit, such as in writing or verbally, or may be implied by conduct.

At or around the time that personal information is collected, staff of the Archdiocese should take reasonable steps to bring this Policy to the individual's attention. Once an individual is made aware of this Policy, it will be assumed that the individual has read and agrees to the terms of the Policy unless the individual informs the Archdiocese of any specific objections or

his or her non-consent in writing.

4.4 Collecting sensitive information
If sensitive information is to be collected, then not only is the collection required to be reasonably necessary for the Archdiocese's entity's functions or activities, the individual about whom the sensitive information relates must also consent to the collection. The relevant exceptions to these requirements are:

- If the collection is authorised by law;
- if a permitted general situation exists (see definition in section 1); or
- (by virtue of the Archdiocese being a non-profit organisation) if the information relates to the activities of the Archdiocese and the information relates solely to the members of the organisation or individuals who have regular contact with the organisation (e.g. collection of information through a survey of the views on religious or moral issues of members of a local parish).

The above means that, unless a relevant exception is applicable, sensitive information must be collected from the individual directly. The individual can consent for his or her information to be obtained from someone else, e.g. a person can give consent for his or her medical records to be obtained from his or her doctor.

4.5 Collection must be by lawful and fair means
Collection of personal information must be lawful. Furthermore, it must be fair, meaning it must not involve intimidation or deception and is not unreasonably intrusive. What is fair would depend on the circumstances.

Examples of unfair collection could include:

- Misrepresenting the purpose or effect of collection, or consequences for the individual if the information is not provided;
- collecting from an unattended or lost electronic device;
- collecting from a traumatised, intoxicated or shocked individual;
- collecting in a way that disrespects cultural differences;
- collecting by deception (e.g. wrongly claiming to be a doctor or a trusted organisation).

5.0 APP4 – UNSOLICITED PERSONAL INFORMATION
This principle relates to if the Archdiocese receives unsolicited personal information, being personal information of a person that it had not requested.

When the above occurs, the Archdiocese must first decide whether or not it could have collected the information if it had requested the information (see section 4 above). It must then decide whether or not the information should be destroyed or de-identified or retained.

5.1 Information that the Archdiocese could not have collected
Unsolicited personal information could be information that the Archdiocese could not have collected (i.e. it is not information necessary for the functions and activities of the Archdiocese or consent of the individual would not normally be given). An example of such information could be a letter sent to a parish by mistake.

In such circumstances, the Archdiocese must destroy or de-identify the information as soon

as practicable unless it is unlawful or unreasonable to do so. An example of when it might be unreasonable or unlawful to destroy unsolicited personal information include if the information might indicate criminal activity which should then be passed onto the police.

5.2 Information that the Archdiocese could have collected

The Archdiocese may retain unsolicited personal information if it determines that it could have collected the personal information under APP3 (see section 4 above) or if it is unlawful or unreasonable to destroy or de-identify the information. An example of such information is an unsolicited job application addressed to the Archdiocese which the Archdiocese can use to contact the sender if a suitable position arises.

Such information retained is to be treated as any other piece of collected personal information.

6.0 APP 5 – NOTIFICATION OF COLLECTION OF PERSONAL INFORMATION

When the Archdiocese collects personal information about an individual, reasonable steps must be taken to notify the individual of certain prescribed matters to ensure awareness. The prescribed matters are:

- The Archdiocese' identity and contact details;
- the facts and circumstances of the collection;
- if the collection is required or authorised by law;
- the purpose of the collection;
- the consequences for the individual if the personal information is not collected;
- the identity of other organisations or persons to which the personal information is usually disclosed;
- information about this Policy;
- whether the Archdiocese will likely disclose personal information to overseas recipients, and if so, in which countries.

Staff of the Archdiocese should prepare and provide suitable collection notices when collecting personal information unless it is not reasonable to do so. Notices can be sent in paper-form or be made available online.

Notices are not required to be provided if circumstances are unreasonable. Such situations include:

- If the individual is aware that personal information is being collected and of the prescribed matters, e.g. if an administrative staff member of the Archdiocese tells a person that his or her information will be passed onto the parish priest for the purposes of arranging a Church-related event;
- if personal information from an individual is collected on a reoccurring basis;
- if notification could pose a serious threat to life, health or safety of an individual or of the public;
- if notification would be inconsistent with another legal obligation, e.g. the obligation to keep the information confidential;
- if notification is impracticable, e.g. if the personal information of an employee's next of kin is collected for emergency contact reasons, it would be impractical for the Archdiocese to notify the next of kin of the collection.

7.0 APP 6 – USE & DISCLOSURE OF PERSONAL INFORMATION

This principle provides that the Archdiocese can only use or disclose personal information for a purpose for which it was collected (known as the "**primary purpose**"), or for a "**secondary purpose**" if an exception applies.

7.1 Primary purpose

7.1.1 The "primary purpose" is the specific function or activity for which the Archdiocese collects the relevant personal information. Examples include:

- The name and contact details of parishioners are collected for the primary purpose of allowing a parish or the Archdiocese to contact said parishioners from time to time to advise them of parish activities;
- the name, contact details, religious affiliation and other personal information provided by a couple to a priest are collected for the primary purpose of arranging their marriage ceremony;
- the name, contact details and employment history of employees of the Archdiocese are collected for the primary purpose of allowing the Archdiocese to consider and administer the employment of such persons;
- name, date of birth and Working with Vulnerable People registration details or Working with Children Check Number (whichever applicable) are collected for the primary purpose of satisfying the Archdiocese that such persons are legally permitted to work with children and/or vulnerable persons;
- the personal information, including sensitive information (e.g. health records) of retired priests are collected for the primary purpose of allowing the Archdiocese to support and assist such persons in retirement.

7.1.2 Personal information collected for the primary purpose can be used or disclosed for that purpose. A person can consent for their personal information to be collected, used and disclosed for a number of primary purposes. The personal information will be used internally within the Archdiocese (and if necessary, its organisations or agencies such as parishes) by authorised employees and may also be used to contact the individual directly from time to time for the relevant primary purpose.

7.1.3 Personal information should not be used or disclosed for any other purpose unless an exception applies, see below.

7.2 Secondary purpose

7.2.1 A "secondary purpose" is any purpose other than the primary purpose for which personal information is collected. Personal information can only be disclosed for a secondary purpose if an exception below applies:

7.2.2 Using or disclosing information with the individual's consent – an individual can consent (expressly or implicitly) for their personal information to be used for a secondary purpose. For example, a parishioner, who had provided his or her name and email to make an enquiry with a parish, can also give consent for that information to be used to receive marketing materials from the Archdiocese.

7.2.3 Using or disclosing personal information where reasonably expected by the individual and related to the primary purpose of collection – there are two aspects of these exceptions:

- There needs to be a reasonable expectation of the individual of such use; and
- if the information is sensitive information, the secondary purpose has to be directly related to the primary purpose, but if the information is not sensitive information, the secondary purpose must be related to the primary purpose.

An example is that a priest would reasonably expect that his name, contact details and availability may be disclosed by the parish or Archdiocesan office to a person requesting religious counselling, as that is related to the primary purpose being the administration of his parish.

Another example of reasonable disclosure is to third party providers to the Archdiocese (e.g. accountants or IT services), who may have access to and use personal information e.g. to process payroll information or to back up online data. In such circumstances, the Archdiocese will take reasonable steps to ensure that external service providers and third parties only use the personal information for the purpose for which the information was provided and to not share it further with another party unless it is necessary to do so.

- Using or disclosing personal information as required or authorised by law – personal information can be used for a secondary purpose if required or authorised by law. This includes warrants, orders or court notices or if there is a statutory requirement to report (e.g. suspected cases of child abuse).
- Using or disclosing personal information where a permitted general situation exists. We refer to the definition of "permitted general situation" in section 1 above. Use of disclosure of personal information in any of those circumstances will be permitted.

8.0 APP7 – DIRECT MARKETING

8.1 **"Direct marketing"** involves the use of personal information to communicate directly with an individual to promote goods and services. This can be carried out in a variety of ways, including in person, by telephone, SMS, email or online advertising. Personal information must not be used for direct marketing purposes unless in accordance with this APP7.

8.2 The Archdiocese and its organisations and agencies such as parishes may, from time to time, engage in direct marketing activities for various purposes, such as fundraising. Individuals whose personal information is used for direct marketing purposes must reasonably expect that their information would be used for such purposes. For example, a person who signs up for a newsletter would have a reasonable expectation that he or she might receive further news about other Archdiocesan services. On the other hand, a person who provides personal information to lodge a complaint with a parish would not expect that his or her personal information will be used for marketing purposes.

8.3 When the Archdiocese or its agencies engage in direct marketing, it must give the recipient an easy means to opt-out of receiving further marketing materials. There should be a visible, clear and easily understood explanation of how to opt-out. For example, an online newsletter emailed to a person can have a link which a person can click to unsubscribe from that newsletter.

8.4 Once a person has opted-out, their personal information should not be used for future direct marketing activities of which the opting-out relates.

In addition to the requirements of the Privacy Act, the *Spam Act 2003* and the *Do Not Call Register Act 2006* contains additional, related legislation relating to direct marketing.

9.0 APP8 – CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

The Archdiocese must disclose certain matters if any personal information that it handles is disclosed to overseas recipients.

At the date of this Policy, the Archdiocese does not send any personal information it collects, uses or discloses to overseas recipients.

10.0 APP9 – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

10.1 A **"government related identifier"** is a number or letter or a combination of these that have been assigned by a State or Commonwealth authority, which can be personal information. Examples include drivers licence numbers and tax file numbers, but does not include Australian Business Numbers.

10.2 In accordance with this principle, the Archdiocese will not:

10.2.1 Unless it is authorised to do so, use government related identifiers to identify individuals (e.g. identify individuals based on their tax file numbers).

10.2.2 Use or disclose government related identifiers unless one or more of the following exceptional circumstances apply:

- where reasonably necessary to verify the identity of the individual;
- where reasonably necessary to fulfil obligations to a government authority;
- where required or authorised by law or a court/tribunal order;
- where a permitted general situation exists (see definition in section 1 above); or
- where required to be given to an enforcement body for enforcement related activities.

11.0 APP10 – QUALITY OF PERSONAL INFORMATION

11.1 The Archdiocese must take reasonable steps to ensure that the personal information it collects, uses or discloses is accurate, up-to-date and complete.

11.2 Individuals may be asked from time to time to review and update their personal information. Staff of the Archdiocese should use reasonable endeavours to keep accurate

and complete records of personal information where possible. See sections 13 and 14 below in relation to access to and correction of personal information.

12.0 APP11 – SECURITY OF PERSONAL INFORMATION

12.1 The Archdiocese must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure. The personal information held by the Archdiocese may be stored in many forms of media. It may keep copies of correspondence (in physical and/or electronic form) as is necessary to carry out its functions and activities and provide its services and programs.

12.2 The Archdiocese takes the security of personal information seriously. Security measures taken include, but are not limited to, the following:

- All personal information is securely stored at all times by the Archdiocese or an authorised external service provider;
- frequent use of virus scanning tools;
- its computers and servers are protected by secure user IDs and passwords, to help protect it from misuse, unauthorised access, modification or disclosure; and
- only authorised people who need to have access to relevant personal information will have access to it.

12.3 The Archdiocese's websites are linked to the internet, and the internet is inherently insecure. It cannot provide any guarantee regarding the security of transmission of information a person communicates to the Archdiocese online. It also cannot guarantee that the information supplied will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which is transmitted to the Archdiocese online is transmitted at the sender's own risk.

12.4 Once the personal information held by the Archdiocese is no longer needed for any purpose for which the personal information may be used or disclosed, it should be destroyed or deidentified, unless such information is required to be retained by law.

13.0 APP12 – ACCESS TO PERSONAL INFORMATION

13.1 Individuals have a right to access their personal information held by the Archdiocese. Furthermore, as the Archdiocese aims to hold accurate, up-to-date and complete records of personal information, individuals are encouraged to contact the Archdiocese to update their records should they change from time to time.

13.2 The Archdiocese should always confirm the person's identity before giving access to personal information.

13.3 There are circumstances where the Archdiocese will not give a person access to personal information it holds. The grounds on which an organisation can refuse to give access include, of relevance:

- The Archdiocese reasonably believes that giving access would pose a serious threat to the life, health and safety of any individual, or to public health or safety;
- if giving access would have an unreasonable impact on the privacy of other individuals;

- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the Archdiocese and the individual;
- giving access would reveal the intentions of the organisation in relation to the negotiations with the individual in such a way as to prejudice the negotiations;
- giving access would be unlawful;
- denying access is required or authorised by law or a court/tribunal order;
- the Archdiocese has reason to suspect that unlawful activity or misconduct of a serious nature that relates to the Archdiocese's function or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by or on behalf of an enforcement body; or
- giving access would reveal evaluative information generated within the Archdiocese in connection with a commercially sensitive decision-making process.

13.4 Subject to the above, there is usually no cost for accessing the personal information held by the Archdiocese, unless the request is complex or resource intensive. If there is a charge, it will be reasonable and the Archdiocese will let the individual know what it is going to be so that he or she can agree to it before access is arranged.

13.5 The Archdiocese will respond within 30 days after a request for access is made by either agreeing to or refusing to give access.

14.0 APP13 – CORRECTING PESONAL INFORMATION

14.1 The Archdiocese is required to take reasonable steps to correct personal information to ensure that the information it holds is accurate, up-to-date, complete, relevant and not misleading.

14.2 If an individual needs to contact the Archdiocese for any reason in relation to this Policy or his or her personal information (whether it be to update their information, access their information, ask a question about how the Archdiocese handle personal information, make a comment about this Policy or to make a privacy complaint), the individual can contact the Archdiocese by contacting the Chancellor (02) 62399871; GPO Box 3089 Canberra ACT 2601.

14.3 If an individual makes a complaint about privacy, the Archdiocese will acknowledge receipt of the complaint, and try to investigate and respond to the person within 30 days. If the individual is unhappy with the outcome, he or she can lodge a complaint with the Office of the Australian Information Commissioner.

15.0 PRIVACY ACT EXEMPTION - EMPLOYEES

15.1 Pursuant to the Privacy Act, the handling of personal information of employees of the Archdiocese is exempt from the Privacy Act (including the APPs discussed above), if the act is directly related to:

15.1.1 A current or former employment relationship between the legal employer and the individual; and

15.1.2 an employee record held by the employer and relating to the individual.

15.2 An "employee record" is a record of personal information relating to the employment of the individual, and it includes information such as the engagement, training, discipline or resignation of the employee, the employees performance, conduct, salary or wage, as well as the employee's health information.

The above means that the relevant legal employer in the Archdiocese is, for example, not required to give its employees access to employee records it holds in respect of that individual. The relevant legal employer may also collect or disclose personal information of its employees, provided that it directly relates to the current or former employment relationship between the employer and the individual.

The exemption will not apply in the following circumstances:

15.2.1 If the act is not directly related to the current or former employer relationship, e.g. the Archdiocese cannot sell a list of employee records or otherwise use such information for commercial purposes unrelated to the employment context; and

15.2.2 if the records do not relate to a current or former employee, e.g. the exemption will not apply to records held of unsuccessful job applicants or persons who have not yet commenced employment with the Archdiocese.

16.0 MANDATORY REPORT REQUIREMENTS

Persons who work with children and/or vulnerable people in NSW and the ACT are required to comply with the relevant legislation in relation to mandatory reporting.

16.1 Australian Capital Territory

16.1.1 Pursuant to the Children and Young People Act 2008 (ACT) (ACT Care Act), certain persons working or volunteering in the ACT are required to report suspected cases of sexual abuse or non-accidental physical injury of a child or young person (being a person under the age of 18) to the Care and Protection Services Centralised Intake Service.

16.1.2 Section 356 of the ACT Care Act sets out the classes of people who are "mandatory reporters" and includes teachers, counsellors and childcare operators.

16.1.3 If a mandatory reporter has reasonable grounds to suspect that a child or young person is at risk of sexual abuse or non-accidental physical injury and those grounds arise during the course of or from the person's work, the person normally has a duty to report, as soon as practicable, to the Care and Protection Services Centralised Intake Service information relating to the child and grounds for the suspicion.

16.2 New South Wales

16.2.1 Pursuant to the Children and Young Persons (Care and Protection) Act 1998 (NSW) (NSW Care Act), certain persons are required to report suspected cases of child abuse and neglect to Family and Community Services.

16.2.2 Section 27 of the NSW Care Act sets out the classes of people who are "mandatory reporters". They include those persons who work directly with children (such as teachers, doctors, therapists, psychologists, counsellors, principals and child care workers) and persons who hold management positions in organisations the duties of which are directly responsible for, directly supervise or provide services to children, such as business managers, officers and directors of such organisations.

16.2.3 If a mandatory reporter has reasonable grounds to suspect that a child or young person (being persons under the age of 18) is at "risk of significant harm" and those grounds arise during the course of or from the person's work, the person has a duty to report, as soon as practicable, to Family and Community Services the name or description of the child and grounds for the suspicion.

16.2.4 Pursuant to section 23 of the NSW Care Act, there are numerous circumstances that constitute "risk of significant harm" to a child or young person, including but not limited to neglect, actual or risk of physical or sexual abuse, caregivers not arranging for the child or young person to be educated, behaviour of caregivers towards the child or young person that could cause or has caused serious psychological harm and a child or young child at risk of serious physical or psychological harm due to domestic violence.

16.2.5 Mandatory reporters should acquaint themselves with the Mandatory Report Guide for further information.

17.0 REPORTING TO THE OMBUDSMAN

17.1 Organisations within NSW and the ACT that provide services to children (including the Archdiocese, its schools and agencies) have additional reporting requirements to their corresponding Ombudsman pursuant to the Ombudsman Act 1989 (ACT) for ACT and the Ombudsman Act 1974 (NSW) for NSW. These entities are called "designated nongovernment agencies" in the NSW Act and "designated entities" in the ACT Act. For the purposes of this Policy, we will refer to them as "designated entities".

17.2 Designated entities are required to notify the relevant Ombudsman in their state or territory about reportable allegations and reportable convictions against employees (including volunteers). "Reportable allegations" are allegations of reportable conduct that include a sexual offence committed against or in the presence of a child (including offence involving child abuse material), assault, ill-treatment, neglect or behaviour that causes psychological harm towards a child and reportable convictions are convictions of an offense involving such conduct.

17.3 Reportable conduct does not include reasonable discipline, management or care of a child.

17.4 Notification to the ACT or NSW Ombudsman (as the case may be) of any reportable allegation or conviction involving an employee must be carried out as soon as possible, but no later than 30 days after the designated entity. The designated entity must also investigate any allegations of reportable conduct and provide a final report to the relevant Ombudsman.

We refer to publications available on the NSW and ACT Ombudsman websites for more information in relation to notifying and identifying reportable conduct.

17.5 **Relationship with the Privacy Act**
Collection, use and disclosure of personal information for reporting purposes pursuant to the NSW Care Act, the ACT Care Act, the relevant Ombudsman legislation, as well as reporting for other lawful reasons (e.g. to the police to report a crime) will not breach the Privacy Act.

18.0 INFORMATION SHARING
Staff of the Archdiocese may share information internally, with another Catholic organisation or the public in accordance with the following principles:

18.1 The Archdiocese takes seriously the requirements of the Privacy Act in relation to the protection of personal information, in particular, sensitive information.

18.2 A general rule is that personal information is only to be shared if the person to which the information pertains has consented to the disclosure and the disclosure is for the primary purpose for which it was collected (see section 7.1 above).

18.3 In some instances, exceptions to the above may apply, and personal information may be disclosed for a secondary purpose (see section 7.2 above), including if the secondary purpose is related to the primary purpose and the person would reasonably expect the disclosure, or if there is a permitted general situation where disclosure is permissible (e.g. if required by law).

18.4 Where personal information is to be disclosed, the Archdiocese will only disclose the relevant and necessary information and not more than what is required in the particular circumstances.

18.5 Disclosure may be required by laws outside the Privacy Act, for example, mandatory reporting pursuant to the Care Act (see section 16 above), or other legislation, such as mandatory financial reporting or reporting to the Australian Charities and Not-for-Profits Commission.

18.6 The Archdiocese reserves the right to refuse to share certain personal information if the sharing of such information would contravene the Privacy Act, or any other law, or if the information is required to be kept confidential for any other reason (e.g. pursuant to a binding contract or confidentiality agreement).

18.7 Where another privacy policy applies in relation to the collection, use or disclosure

of personal information in specific circumstances (e.g. the privacy policy of the Catholic Education office in relation to personal information about a school student, or the privacy policy of a retirement village in relation to personal information of a resident), staff should be guided by the terms of that document.

19.0 NOTIFIABLE DATA BREACHES

On and from 22 February 2018, where a notifiable data breach occurs, the Archdiocese is required to notify the Office of the Australian Information Commissioner and any individuals likely to be at risk of serious harm by a data breach.

19.1 Key concepts

A "notifiable data breach" is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

19.1.1 A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure, e.g. if a device containing personal information is lost or stolen, if servers containing such information are hacked or if personal information is mistakenly provided to the wrong person.

19.1.2 "Serious harm" is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

19.1.3 Not all data breaches are eligible. For example, if the breach is quickly rectified and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify.

19.2 Assessment of breach

In determining whether a reasonable person would conclude that the breach would cause serious harm to individuals to which the information relates, the Archdiocese will assess the risk of serious harm holistically, having regard to the likelihood of the harm eventuating for individuals whose personal information was part of the data breach and the consequences of the harm. The Archdiocese will have regard to the following:

19.2.1 The kind or kinds of information;
19.2.2 the sensitivity of the information;
19.2.3 whether the information is protected by one or more security measures;
19.2.4 if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome;
19.2.5 the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
19.2.6 if a security technology or methodology: 19.2.7 was used in relation to the information; and
19.2.8 was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information the likelihood that the persons, or the kinds of persons, who:
19.2.9 have obtained, or who could obtain, the information; and
19.2.10 have, or are likely to have, the intention of causing harm to any of the

individuals to whom the information relates;
19.2.11 have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;
19.2.12 the nature of the harm;
19.2.13 any other relevant matters.

19.3 Response to data breach
There is no single way to respond to a data breach given the wide variety of circumstances under which a breach can occur. The four key steps to consider when responding to a breach or suspected breach are (in order):

19.3.1 Contain the breach and do a preliminary assessment;
19.3.2 evaluate the risks associated with the breach;
19.3.3 notification; and
19.3.4 prevent future breaches.

19.4 Notification
If the Archdiocese has reasonable grounds to believe there has been a notifiable data breach, it must promptly prepare a statement for the Commissioner and make a prompt decision about which individuals to notify.

There are three options for notifying individuals at risk of serious harm, depending on what is practicable for the Archdiocese in the circumstances:

19.4.1 Option 1 – notify all individuals to whom the relevant information relates. This option would be the most practicable if it cannot be easily assessed which particular individual are at risk of serious harm;
19.4.2 Option 2 – notify only those individuals at risk of serious harm; or
19.4.3 Option 3 – if neither option 1 or 2 are practicable, the Archdiocese must publish a copy of the statement on its website and take reasonable steps to publicise the contents of the statement.

20.0 CHANGES TO THIS POLICY
This Policy was last updated on 15 September 2017.

If this Policy changes, the revised Policy will be posted on the Archdiocesan website at http://cgcatholic.org.au and will be available from the Chancery office at 55 Franklin Street, Forrest ACT.

This Policy supersedes all previous policies relating to matters contained therein.