**1. Background**

The Australian Parliament passed the Privacy Act 1988 (Privacy Act) at the end of 1988, and it commenced in 1989. The Act was amended by the Privacy Amendment (Private Sector) Act 2000 (commenced 21 December 2001) which extended coverage of the Privacy Act to some private sector organisations. These amendments also introduced 10 National Privacy Principles into the Privacy Act, which set standards for private sector organisations when they collect, use and disclose, hold secure, give access to, and correct personal information. Further major amendments were made under the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (commenced 12 March 2014), which introduced the Australian Privacy Principles (APP’s) and extended the powers of the Australian Information Commissioner (AIC).

In general the legislation requires organisations to comply with the APP’s (set out in Schedule 1 of the Privacy Act 1988). These principles provide for the collection, use, disclosure and management of personal information by organisations. For these purposes "personal information" means any information, including an opinion, about a person that can be used to identify the person, for example a person's name or address. It will also include a picture of a person.

Small businesses are generally exempt from the legislation. A small business is a business which has an annual turnover of less than $3 million. A small business can lose its exemption from the legislation for a number of reasons. If a small business loses its exemption it will then have to start complying with the legislation. The AIC’s Office has indicated that organisations such as parishes should be regarded as small businesses for the purposes of the small business exemption under the legislation.

Regardless of any exemption a parish may have from the legislation, there are increasing expectations in the community in relation to privacy generally. If a person has a genuine grievance about the way in which a parish has handled his or her personal information, it is unlikely that the grievance will be satisfactorily resolved by relying on an exemption from the legislation. While reliance on an exemption may mean the parish avoids the risk of a financial penalty for a breach of privacy under the legislation, a grievance which is not satisfactorily resolved may lead to damaged relationships which, in serious cases, may affect the mission of the parish.

In view of these matters, the Diocesan Registry encourages parishes to review their approach to privacy with 2 objectives in mind:

(a) First, to ensure that parishes retain the benefit of the small business exemption under the legislation.

(b) Second, to minimise the risk of complaints being made about perceived or actual breaches of privacy regardless of any exemption from the legislation.

**2. Small business exemption**

*2.1 How can a parish lose its small business exemption?*

A parish can lose its exemption from the legislation as a small business if it -

(a) exceeds an annual turnover of $3 million in the previous financial year, or

(b) is a health service provider, or

(c) trades in personal information (eg buying or selling a mailing list), or

(d) is a contractor that provides services under a Commonwealth contract; or

(e) is a reporting entity for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act); or

(f) operates a residential tenancy database; or

(g) is a credit reporting body; or

(h) is an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009; or

(i) is a business that conducts protection action ballots; or

(j) is a business related to a business that is covered by the Privacy Act; or

(k) is a business prescribed by the Privacy Regulation 2013. or

(l) is a business that has opted in to be covered by the Privacy Act.

Most of these will not apply to parishes, however some possibilities are discussed in more detail below.

*2.2 Exceeding the $3 million annual turnover threshold*

A parish can lose its small business exemption if its annual turnover in the previous financial year exceeds $3 million.

A review of the turnover of our parishes indicates that no parish met (or is approaching) this threshold. Accordingly, it is unlikely that any parish will lose its small business exemption in the near future by reason of exceeding the $3 million annual turnover threshold.

*2.3 Being a health service provider*

A parish can lose its small business exemption if it provides a health service and holds health information (except health information in an employee record), even if that is not its principal activity.

A health service includes an activity which is intended or claimed to assess, record, maintain, improve or manage a person’s physical or psychological health; or to diagnose or treat an individual's illness or disability. Although parishes do not generally provide health services to individuals, activities such as counselling may constitute the provision of a health service depending on the nature of the counselling.

To lose its exemption, the parish must also hold health information (except in an employee record). Health information includes personal information about the health or a disability of an individual or a health service provided, or to be provided, to an individual.

*2.4 Trading in personal information*

A parish is ’trading’ in personal information if they collect or disclose an individual’s personal information to someone else for a benefit, service or advantage. A benefit, service or advantage can be any kind of financial payment, concession, subsidy or some other advantage or service.

Trading in personal information generally means buying, selling or bartering personal information. For example, buying a mailing list without first getting the consent of all the individuals on that list, or disclosing customer details to someone else for some commercial gain.

If a business trades in personal information they have to comply with the Australian Privacy Principles in the Privacy Act 1988.

A business is **not** trading in personal information if they give or receive personal information for a benefit, service or advantage and they:

* have the consent of all the individuals concerned, or
* only do so when authorised or required by law

For example, if a parish sells the personal information contained in a parish directory, it is likely that the parish will lose its small business exemption unless each individual named in the directory has consented to the parish disclosing the information in this way. A parish may also trade in personal information if it charges a fee for personal information contained in a church register. Again, it is likely that the exemption will be lost unless the individual(s) concerned have consented to the disclosure (see 3.6 for information about church registers and records).

*2.5 Being a contracted service provider under a Commonwealth government contract*

Another way in which a parish can lose its small business exemption is if it is a contracted service provider for a Commonwealth government contract. This will occur if a person acting on behalf of the parish is a party to (or a subcontractor under) a Commonwealth government contract which involves the provision of services to a Commonwealth government agency.

*2.6 Suggested action to avoid losing the small business exemption*

It is suggested that parishes review their activities in light of the matters raised above to identify whether any activity puts the parish at risk of losing its small business exemption. If such a risk is identified it is suggested that, where possible, the parish ceases the activity or modifies the activity to the extent necessary to minimise the risk.

In some cases a parish may identify a risk activity but may take the view that it is not possible or appropriate to cease or modify the activity in order to avoid the risk of losing its small business exemption. In this case a parish may need to go beyond the suggestions regarding good privacy practice set out in the remainder of this circular and adopt more formal procedures for compliance with the legislation. If this is the case, please contact the Registrar on 6772 4491 for further information.

**3. Good privacy practice**

*3.1 Privacy principles*

Organisations which are bound by the legislation are required to handle personal information in accordance with the APP’s. While the APP’s may not be legally binding on parishes, they nonetheless reflect good privacy practice. Parishes are therefore encouraged to review the APP’s and, as far as possible, to implement them in the way they handle personal information. A summary of the APP’s can be found at the end of this Policy.

There are some specific matters that commonly arise from an application of the APP’s in the parish context. These matters relate to -

(a) Compilation and distribution of parish or church directories.

(b) Parish newsletters, rosters and websites

(c) Publication of pictures of individuals.

(d) Personal information held in church offices.

(e) Church registers and archives.

Each of these areas is considered below.

*3.2 Compilation and distribution of church directories*

The compilation and distribution of a parish or church directory is perhaps the most significant way in which a parish handles personal information. Many parishes consider the compilation and distribution of such directories as an important way of facilitating the ministry of the parish. There are however potential privacy risks associated with the use of such directories.

While it is not suggested that parishes should discontinue the practice of compiling and distributing directories, it is suggested that parishes which choose to do so should consider implementing a number of measures aimed at reducing the risk of a complaint being made about the way in which personal information included in the directory is used.

First, the persons included in the directory should, as far as possible, be limited to those persons who are regular members of the church and those who are closely associated with the church or parish.

Second, when compiling the information for the directory, each person whose details are to be included in the directory (including parents on behalf of children) should be asked to consent to their personal details being included in the directory. This could be done by asking each person to fill out the necessary details on a card distributed during or at the end of a church service. Alternatively, each person could be asked to check, update and sign-off on their directory details already held by the parish. The card or the information to be checked should include or be accompanied by a statement to the effect that the person checking or providing the information agrees to the information being included in the church directory to enable members of the church or parish and close associates to contact each other directly.

Third, the directory should be distributed only to those persons who members of the church or parish. Accordingly, it would not be appropriate to make copies of the directory generally available by, for example, having copies available at the back of the church.

Fourth, it may be appropriate to include in the directory a statement to the effect that the directory is being provided to enable regular members of the church or parish and close associates to contact each other directly and that the information in the directory should not be used or disclosed for any other purpose.

Finally, it is suggested that where possible copies of the directory are provided to members and close associates free of charge. This avoids the parish running the risk of losing its exemption from the privacy legislation on the basis of "trading" in personal information. If a parish wishes to charge for a copy of the directory, the charge should be nominal and relate only to the administrative costs of compiling the directory.

*3.3 Parish newsletters, rosters and websites*

Another area of privacy risk for parishes relates to the publication of personal information in parish newsletters, rosters or on parish websites.

If a person provides information on a confidential basis, then clearly the publication of such information, even if well intended, would generally be a serious breach of privacy. On the other hand, if a person provides information about themselves in circumstances where it is clear that the person has agreed or would reasonably expect the information to be published in a particular way, then the publication of information in that way would not generally raise privacy concerns. For example, a person who responds to a general request from the Vicar for volunteers to assist at Sunday School might reasonably expect his or her name to be published on a publicly available roster if at the time the Vicar made the request he also indicated that a roster would be published in this way. The reasonable expectations of the volunteers would be further clarified if the publication of such a roster had been a long standing, widely known and regularly publicised practice in the Parish.

Difficulties may however arise in the following circumstances -

(a) where a person has provided information about themselves but in circumstances where it is not clear that he or she would reasonably expect it to be published in a particular way, or

(b) where a person provides information about another person for publication.

In either of these circumstances it is suggested that confirmation should generally be sought from the person concerned before the information is published.

In particular circumstances confirmation about the publication of personal information provided by one person about another person may not be necessary. For example information which has been provided about a missionary supported by the parish might be published without confirmation if the information is public knowledge or if the missionary has previously agreed to similar types of information being published about them (such as by way of regular report or update). The test in each case is whether the person concerned would reasonably expect the information about them to be published in a particular way and would not otherwise be offended, embarrassed or put in an awkward position by the publication of the information.

Particular care should be taken in relation to sensitive information such as information about health or personal difficulties. Particular care should also be taken in relation to any information to be published on a parish website since a website is accessible to the entire world.

*3.4 Publication of pictures of individuals*

A picture of a person is personal information for the purposes of the privacy legislation. In deciding whether to publish a picture of a person, similar considerations to those raised in relation to the publication of personal information in a parish newsletter or roster or on a parish website should be adopted.

While it is generally desirable to obtain the consent of each person (or parent on behalf of a child) before publishing his or her picture in a parish document or on a parish website, it may not be practical to do so in relation to pictures of large groups where no person is featured. In this case it would generally be adequate to inform the group of the parish's intention to publish the picture and give the persons in the group a reasonable time to object to their picture being published.

Clearly, pictures which are sensitive or are likely to cause embarrassment or awkwardness should not be published under any circumstances (eg certain photographs from church camps or houseparties). Particular care should also be taken in relation to pictures of children.

*3.5 Personal information held in church offices*

Staff and others working in church offices should consider the following when handling personal information:-

(a) Personal information held in the office should be provided only to members of the ministry team or support team, and only when necessary for ministry purposes. Personal information held in the office should not be provided to any other person, without the prior consent of the person concerned.

(b) Staff should ensure that any personal information obtained during the course of their work is used only for the purposes of the parish and in a way that the persons concerned would reasonably expect (see 3.3 and 3.4). Where the reasonable expectations of a person are not clear, confirmation about the use should generally be sought from the person.

(c) If the office receives a request, for example by telephone, to provide personal information about a church member etc, the office should take the contact details of the person making the request and pass the contact details onto the church member to allow the church member to make direct contact with the person.

(d) Those working in the office should not assume that everybody who has access to the office is entitled to have access to all personal information held in the office. In particular they should -

* keep documents and computers containing personal information reasonably secure (eg by using logins and passwords for computers and locked cabinets for paper records)
* keep personal information reasonably up-to-date
* destroy documents containing personal information when they are no longer needed (eg using a shredder or security bin).

They should not -

* make unnecessary copies of documents containing personal information
* leave documents lying around the office where those who should not see them can do so
* share login details or passwords to computers

(e) A person's details should be removed from any mailing list used by the office if the person requests the office to do so (ie a person should not be contacted if he or she doesn't want to be contacted).

(f) Church offices should allow persons to have access to any information held about them in the office, for example to update or check the accuracy of the information. This would generally need to be done in person to ensure that access is given only to the person about whom the information relates.

*3.6 Church registers and archives*

Parishes should consider limiting the provision of an extract from a church register involving a baptism, confirmation or marriage which took place in the last 70 years to the person(s) about whom the information relates. There is generally no such restriction on the release of information about funerals since privacy considerations do not directly apply to deceased persons.

Any fee charged for providing an extract from a church register should be reasonable and limited to the administrative costs of providing the information. It would be preferable for a parish to provide extracts from its church registers free of charge where, for example, the frequency of requests for such information is low. This removes any risk of the parish losing its small business exemption from the legislation on the basis that the parish is "trading" in personal information.

The management of church registers and archives for privacy purposes is a specialised area. It is suggested that parishes contact the Registrar on 6772 4491 or at registrar@armidaleanglicandiocese.com for more specific guidance as to the way in which church registers and archives should be handled in view of the privacy legislation.

Please call the Registrar on (02) 6772 4491 if you wish to discuss any matter raised in this circular.

Christopher Pears, Registrar

**Summary of Australian Privacy Principles (Schedule 1 of the Privacy Act 1988)**

(for more detailed information – refer to the Privacy Fact Sheet 17 at - [https://webarchive.nla.gov.au/awa/20181010003033/https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles](https://webarchive.nla.gov.au/awa/20181010003033/https%3A//www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles) )

*APP 1 — Open and transparent management of personal information*

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

*APP 2 — Anonymity and pseudonymity*

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

*APP 3 — Collection of solicited personal information*

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

*APP 4 — Dealing with unsolicited personal information*

Outlines how APP entities must deal with unsolicited personal information.

*APP 5 — Notification of the collection of personal information*

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

*APP 6 — Use or disclosure of personal information*

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

*APP 7 — Direct marketing*

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

*APP 8 — Cross-border disclosure of personal information*

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

*APP 9 — Adoption, use or disclosure of government related identifiers*

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

*APP 10 — Quality of personal information*

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

*APP 11 — Security of personal information*

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

*APP 12 — Access to personal information*

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

*APP 13 — Correction of personal information*

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