



Anglican Church Diocese of Sydney

St Andrew's House
Sydney Square
New South Wales
Australia

PO Box Q190
QVB Post Office NSW 1230

Telephone: 61 2 9265 1555

Facsimile: 61 2 9261 4485

Privacy Legislation - managing its impact on parishes – 4 November 2002

- **Background**
- **Small business exemption**
 - How can a parish lose its small business exemption
 - Exceeding the \$3 million annual turnover threshold
 - Providing a health service and holding health information
 - Disclosing personal information for a benefit etc
 - Collecting personal information by providing a benefit etc
 - Being a contracted service provider under a Commonwealth government contract
 - Suggested action to avoid losing the small business exemption
- **Good privacy practice**
 - Privacy principles
 - Compilation and distribution of church directories
 - Parish newsletters, rosters and websites
 - Publication of pictures of individuals
 - Personal information held in church offices
 - Church registers and archives
- **Summary of Privacy Principles**

1. Background

As you will be aware, Commonwealth privacy legislation commenced operation on 21 December 2001.

In general the legislation requires organisations to comply with a series of privacy principles set out in the legislation. 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. However if a small business loses its exemption it will not generally have to start complying with the legislation until 21 December 2002. The Federal Privacy Commissioner'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, this circular encourages parishes to review their approach to privacy with 2 objectives in mind.

(a) First, to enable parishes, where possible, to modify the way they handle personal information in order to retain the benefit of the small business exemption under the legislation.

(b) Second, to enable parishes, where possible, to adopt good privacy practice in the way personal information is handled 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) provides a health service and holds any health information (except in a employee record), or

(c) discloses personal information about an individual for a benefit, service or advantage (except with the consent of the individual or as required or authorised by law), or

(d) provides a benefit, service or advantage to collect personal information about an individual from anyone else (except with the consent of the individual or as required or authorised by law), or

(e) is a contracted service provider for a Commonwealth government contract.

Each of these is discussed in more detail below.

2.2 Exceeding the \$3 million annual turnover threshold

A parish can lose its small business exemption after 21 December 2002 if its annual turnover in the previous financial year exceeds \$3 million.

The annual turnover of a parish broadly corresponds to the adjusted receipts for the parish as provided by each parish in its annual financial return. A review of the adjusted receipts for all parishes indicates that no parish had adjusted receipts in 2001 of more than \$1.4 million.

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 Providing a health service and holding health information

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). The exemption can be lost for this reason at any time after 21 December 2001.

A health service includes an activity which is intended or claimed to assess, record, maintain or improve an individual's 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 Disclosing personal information for a benefit etc

A parish can lose its small business exemption after 21 December 2002 if it discloses personal information about another individual to anyone else for a benefit, service or advantage. This does not apply if the personal information is disclosed with the consent of the individual or as required or authorised by law.

Disclosing personal information for a benefit, service or advantage is generally referred to as "trading" in personal information. This will most commonly involve selling personal information for monetary payment. 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 Collecting personal information by providing a benefit etc.

A parish can also lose its small business exemption after 21 December 2002 if it provides a benefit, service or advantage to collect personal information about another individual from anyone else. This does not apply if the personal information has been collected with the consent of the individual or as required or authorised by law.

This is another form of "trading" in personal information and would include a parish paying a person or organisation to provide personal information about other individuals. The circumstances in which a parish might purchase personal information in this way are not immediately apparent.

2.6 Being a contracted service provider under a Commonwealth government contract

The final way in which a parish can lose its small business exemption after 21 December 2002 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.

2.7 Suggested action to avoid losing the small business exemption

It is suggested that parishes review their activities in light of the 5 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 Legal Officer on 9265 1671 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 a series of privacy principles under the legislation. While the privacy principles may not be legally binding on certain parishes, they nonetheless reflect good privacy practice. Parishes are therefore encouraged to review the principles and, as far as possible, to implement them in the way they handle personal information.

A summary of the privacy principles is attached to this circular.

There are some specific matters that commonly arise from an application of the privacy principles 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 whose details appear in the directory. 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 Youth Worker 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 Youth Worker made the request the Youth Worker 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 the staff responsible for the persons concerned. Personal information held in the office should not be provided to any other person.

(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 document 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

Clause 19(4) of the [Church Administration Ordinance 1990](#) provides that a minister may make a search on and furnish an extract from a church register on the application of any person and on the payment of a reasonable fee. However in view of the privacy legislation (and in accordance with archival practice), 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 Diocesan Archivist, Dr Louise Trott on 9221 0640 or at archives@sydney.anglican.asn.au for specific guidance as to the way in which church registers and archives should be handled in view of the privacy legislation.

Please call the Legal Officer on (02) 9265 1671 if you wish to discuss any matter raised in this circular.

ROBERT WICKS

Legal Officer

Summary of Privacy Principles

1. Collection

1.1 An organisation should generally collect only the personal information it needs for its legitimate functions and activities. The organisation should collect the information in a fair and lawful way.

1.2 Where reasonably practicable an organisation should collect personal information directly from the individual. The organisation should usually take reasonable steps, when collecting information, to ensure that the individual knows why the information is being collected, who the information will be given to and how the information will be used or disclosed, as well as how to contact the organisation and that the individual may access the information. This is the case whether the organisation collects personal information from the individual or from someone else.

1.3 An organisation should usually ensure it has the consent of the individual to collect sensitive information. Sensitive information is information or an opinion about a person's -

- religious or philosophical beliefs and affiliations,
- racial or ethnic origin,
- political opinions or membership of a political association,
- membership of professional or trade associations or a trade union,

- sexual preferences or practices,
- criminal record, or
- health.

2. Use and disclosure

An organisation should usually only use or disclose personal information for -

- the primary purpose for which it was collected,
- a related purpose which the individual would reasonably expect, or
- with consent.

3. Data quality

An organisation should take reasonable steps to introduce systems to ensure that personal information it holds is accurate, current and complete.

4. Data security

4.1 An organisation should implement measures to protect personal information from misuse, loss and unauthorised access, changes or disclosure.

4.2 An organisation should usually destroy or permanently de-identify personal information when the organisation no longer needs it.

5. Openness

An organisation should be open about how it manages personal information. If asked, an organisation should provide information about its approach to privacy.

6. Accessing and correcting personal information

6.1 Usually, when asked, an organisation should give an individual access to their personal information unless there is a reason why the organisation cannot do so. An organisation may deny a request for access if it reasonably believes any of the following circumstances apply -

- it would pose a serious and imminent threat to the life or health of any person, or if health information, would pose a serious threat to the life or health of any person,
- the privacy of others would be unreasonably affected,
- the request is frivolous or vexatious,
- the information relates to existing or anticipated legal proceedings with the person who is the subject of the information and would not be accessible in those proceedings,
- providing access would prejudice negotiations with the person who is the subject of the information by revealing the organisation's intentions regarding those negotiations,
- providing access would be unlawful or denying access is required or authorised by law,
- providing access would be likely to prejudice an investigation of possible unlawful activity,
- providing access would be likely to prejudice law enforcement, public revenue protection, prevention and remedying of seriously improper conduct, or preparation or conduct of court or tribunal proceedings, either by or on behalf of an enforcement body,
- an enforcement body performing a lawful security function requests denial of access to protect national security, and

- where evaluative information generated by the organisation in making a commercially sensitive decision would be revealed by providing access. In this situation the organisation may provide an explanation for the commercially sensitive decision instead.

6.2 The organisation should usually correct personal information if the individual to whom it relates can establish that the information is not accurate, current and complete.

6.3 An organisation should not impose an excessive charge for access by an individual to their personal information.

7. Identifiers

An organisation should generally not adopt, use or disclose Commonwealth government identifiers unless specifically permitted to do so. Identifiers include tax file numbers or social security numbers, but not an ABN.

8. Anonymity

If reasonably possible, an organisation should give others the option of dealing with it anonymously.

9. Transborder data flows

An organisation should generally obtain consent to transfer information overseas unless otherwise permitted to do so.

10. Sensitive information

An organisation should generally obtain consent to collect sensitive information unless otherwise permitted to do so.