British Columbia's *Personal Information Protection Act*
Frequently Asked Questions

1. What is the *Personal Information Protection Act*?

The *Personal Information Protection Act* (PIPA) SBC 2003 c. 38 is a provincial law whose purpose is to govern the collection, use and disclosure of personal information by organizations. The Act recognizes the right of individuals to protect their personal information, and the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. PIPA is distinct from the federal law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which does not apply to communities of faith within British Columbia.

2. Does a local community of faith come under this Act?

Communities of faith must comply with the Act. All non-public organizations within B.C. from the largest corporation to the smallest non-profit society must comply with the Act. It is estimated that 400,000 organizations within B.C. come under PIPA. In provinces that have a Personal Information Protection Act, the provincial act takes precedence over the federal act.

3. What is Personal Information?

Personal information is any factual or subjective information about an identifiable individual and includes:

Home address	Mental/physical disability
Home phone number	Family members names
Age, date of birth	Employee files
Personal email address	Identification numbers: e.g. Social Insurance, Provincial Health, or Drivers Licence numbers
Race	Evaluations
Weight/Height	Income
Colour	Credit card and/or bank records
Religion	Donation information
Sexual orientation	Loan or medical records, etc.
Marital and/or social status	Affiliations

Updated Jan. 2019

4. What is *not* personal information?

Personal information does not include your "business" job title, telephone number, address or email address if you are an employee of the church, or anything that can be found through publicly available information such as the phone book.

5. What is the intent of the PIPA legislation?

The intent of the legislation is to prohibit the use of personal information for both commercial and non-commercial purposes. It is also intended that the legislation will provide a safeguard against identity theft. The federal legislation (PIPEDA) has a narrower standard, being limited to commercial activity, while the B.C. provincial Act (PIPA) also relates to non-commercial activity.

6. If there is a federal act, why do we not simply use that?

In provinces that have privacy legislation, the provincial legislation generally takes precedence over the federal legislation, when the provincial legislation is seen to be "substantially similar" by the office of the Privacy Commissioner of Canada. Thus at the level of community of faith, we need to use the provincial legislation.

7. Does the Pacific Mountain Regional office need to use the provincial or the federal legislation?

This is not as clear. Given that the Region has much to do with personal information that is moved between several legal jurisdictions, it may be that it will have to comply with both provincial and federal legislation. Many inter-jurisdictional issues require further definition and interpretation. The General Council offices follow the federal legislation, in part because Ontario has not yet framed its provincial legislation, and in part because much of the personal information at that level is shared among various legal jurisdictions.

8. Is complying with the privacy legislation a lot of work?

Most communities of faith will not find it difficult. If you haven't already implemented a privacy policy, your community of faith will likely need to pull together a small ad-hoc committee to get your policy launched. The staff, including ministry personnel, will need to become familiar with the privacy policy, and become sensitive to those times when the work of the community of faith is raising privacy issues. A Privacy Officer will need to be appointed. Part of the work of the Privacy Officer is to help the community of faith and its staff keep on top of privacy issues.

9. We have church directories containing the names, addresses and other means of contacting members of the community of faith. Does this infringe on the privacy legislation?

While church directories were originally compiled as an internal reference for members of the community of faith, the statute includes as personal information the items included in the answer given to Question 3. It would be unwise in any event to include most of the information set out in Answer 3 in such directories. If you include home addresses, telephone numbers, e-mail addresses along with the names of members and adherents, you should have the consent of such folks before printing and distributing a directory.

When a new edition is being prepared for publication, members and adherents should be asked to inform those preparing the directory if they do not wish this information to be included.

It is especially important to obtain written consent from members or adherents if you plan to include them in an online directory.

In view of the church's policies concerning the protection of young people within the community of faith's care, it is not advisable to include in the listing in the directory the names and other information, such as e-mail addresses, of any minors. Since minors (under 19 years in B.C.) cannot give their own consent and are persons considered at risk for which the church must provide protection, their names should be excluded from a general church directory.

It is also wise to place a notice inside the front cover of the directory stating that it is published for the use of the community of faith and is not to be circulated to third parties outside of that community. For online directories, it is wise to build in password protection.

10. Can we circulate the names and addresses or e-mail addresses of individual committees for their own use?

This is also personal information that requires the consent of individual members of the committee. What is often done is for the members of a church committee to all agree at the beginning of the committee's work that such a list be prepared, that all *agree* to include names, phone numbers, fax numbers or whatever information seems necessary for the committee's work and that it be kept by each member confidentially.

11. Are minutes of meetings considered to be personal information?

Church board and committee minutes are not confidential. The Manual specifically refers to confidentiality of proceedings of the Ministry and Personnel Committee of the community of faith, and these should not be circulated beyond the membership of that committee. Minutes should not contain any of the personal information set out in Answer 3 and normally would not if they are to be made public. There may be times when church meetings need to go *in camera* to deal with sensitive personnel and other matters. This

should be noted in the minutes, as should any decisions or motions passed in such an *in camera* committee of the whole.

Circulation of minutes of a church court on an Internet website is not encouraged.

12. Do we need to have a Privacy Officer in each community of faith?

Yes. Someone in each community of faith should be so designated.

13. What do we do with records containing personal information?

Records held in the church containing personal information should be kept in a locked and secure area.

14. Who should we name as our "Privacy Officer"?

In most communities of faith, it is likely that the Privacy Officer will not be very busy after the initial planning and "launch" of the privacy policy. It may well be a position that a volunteer could take on, if they were familiar with the life and the organization of the community of faith, and if they are seen as fair minded mediators. In some cases, it may be that an administrative support staff person or church administrator would have the skills and aptitudes required. If no one else is able or willing to accept the position, the position would fall to the ordained minister of the community of faith by default.

15. What do I do if I want to have access to my personal information?

A signed, detailed request should be sent to the Privacy Officer of the community of faith.

16. Can we use the personal information we have on hand for something other than the original reason for which it was collected?

No. The church would have to obtain the consent of the member every time the personal information was to be used for a different purpose. If, however, the personal information is transferred to the Regional Archives, it can be used for archival or research purposes.

Included in the purposes for which personal information is collected are archival or research purposes, based on the long-term or perpetual legal and business purposes of the community of faith.

17. Communities of faith frequently take photos or videos of events which are then posted in bulletins, on websites, etc. Is consent required by anyone whose photo is so published?

Yes. Written, verbal, or tacit consent is required. This is important if the intent is to publish the photos either in print or electronically. There may also be copyright restrictions.

18. Our community of faith has a website, and on it we have a Prayer Concerns List. This gives the names of members of our community who are sick, so that people can pray for their healing or recovery. The list has proven to be very helpful, and includes the specific conditions and ailments that we wish to raise up to God.

The problem is not whether God hears your prayers. The problem is whether others read of your prayer concerns in a published form. Medical personal information is one of the most sensitive kinds of personal information, and specific names and medical conditions should not be disclosed in a written list, whether in a worship bulletin, a website, or any other publication. The disclosure of such sensitive information is not in compliance with the *Personal Information Protection Act*. It would be best to seek a more private forum for such sensitive information sharing, such as within a prayer group. Nor is it prudent to include prayer list information in published worship bulletins. Prayer concerns are best shared verbally in prayer groups or in public worship.

19. Can I refuse to disclose my personal information, and what happens if I do?

You may do so, but it may complicate your life somewhat. If you are a donor to your community of faith, you may wish to have a charitable tax receipt. The church treasurer will need some personal information to provide such a receipt. It is necessary and reasonable for a church organization to require some personal information to carry out its work, for example preparing a pay cheque, processing benefit claims, or managing donor information. At the same time, it is possible to limit the disclosure of certain personal information if you see no benefit in providing it.

20. In Section 35(2) of PIPA, the Act states that: "An organization must destroy its documents containing personal information, or remove the means by which the personal information can be associated with particular individuals, as soon as it is reasonable to assume that (a) the purpose for which the personal information was collected is no longer being served by the retention of the personal information, and (b) retention is no longer necessary for legal or business purposes." Does this affect what records we transfer to our Regional Archives?

No it does not. Communities of faith should continue to send their archival records to the Regional Archives and should use the listing provided in "What the Archives Wants" found in the Toolkit section of the Archives' website at:
https://bc.united-church.ca/sites/default/files/guide.pdf

PIPA is interested in the preservation of archival and historical records for research purposes—even those that contain personal information. In Section 22 of the Act, we are told that: "An organization may disclose personal information for archival or historical purposes if

a) a reasonable person would not consider the personal information to be too sensitive to the individual to be disclosed at the proposed time,
b) the disclosure is for historical research and is in accordance with Section 21 [a section related to the disclosure of personal information for research or

statistical purposes],

c) the information is about someone who has been dead for 20 or more years,
d) the information is in a record that has been in existence for 100 or more years.

Thus Section 22 of the Act does spell out a place for archives. In Section 35(2)(b) we note that the organization must destroy its documents containing personal information only if "retention is no longer necessary for legal or business purposes." It is our interpretation of Section 35(2)(b) that retention of archival and historical records of the organization are included as a part of the ongoing legal or business purposes of the church. Archival records, by their nature, are permanently necessary records for the legal and business purposes of the church.

Finally, in Section 18(1) of the provincial Act, it is stated that "An organization may only disclose personal information if… (n) the disclosure is to an archival institution if the collection of the personal information is reasonable for research or archival purposes…"