



## First Filipino Baptist Church Toronto

382 Lippincott Street, Toronto, Ontario M5S 2P7

Email: [ffbtoronto@bellnet.ca](mailto:ffbtoronto@bellnet.ca), [office@ffbtoronto.org](mailto:office@ffbtoronto.org)

Rev. Eliezer A. Catanus

Pastor Emeritus

Website: [www.ffbtoronto.org](http://www.ffbtoronto.org)

Rev. Rizalino S. Castillo

Associate Pastor

Tel: (416) 534-4342

Fax: (416) 534-5110

Isaac Jordan D. Melis

Associate Pastor

### Personal Information Privacy Commitment Statement

To safeguard the personal information entrusted to the First Filipino Baptist Church Toronto (the "Church") and to comply with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and any other applicable legislation. The Church is committed to the following principles:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

These principles will be enacted in accordance with the Church Policy to Protect Personal Information" (the "Policy"). The Church's directors, officers, employees and volunteers are required to comply with the principles and the Policy and will be given restricted access to personal information solely to perform the services provided by the Church. Other persons or organizations who act for, or on behalf of the Church are also required to comply with the principles and the Policy and will be given restricted access to personal information solely to perform the services provided for the Church.

The Church has designated the existing Chairman and Vice-Chairman of the Board of Directors to be the Personal Information Compliance Officers. Any inquiry, request or concern related to privacy matters should be made in writing to the Church.

Personal Information Compliance Officers  
Board of Directors, Chairman and Vice-Chairman  
First Filipino Baptist Church Toronto  
382 Lippincott Street  
Toronto, Ontario M5S 2P7  
[office@ffbtoronto.org](mailto:office@ffbtoronto.org)

A copy of the Policy is available at the First Filipino Baptist Church Toronto's website:  
[www.ffbtoronto.org](http://www.ffbtoronto.org)

**Policy to Protect Personal Information  
March 2008**

**1. Accountability**

1.1. The existing Chairman and Vice-Chairman of the Board of Directors are hereby appointed as the personal information compliance officers (the “officers”) for the First Filipino Baptist Church Toronto.

1.2. All persons, whether employees, volunteers, or board or committee members who collect, process, or use personal information shall be accountable for such information to the officers.

1.3. This policy shall be made available upon request.

1.4. Any personal information transferred to a third party for processing is subject to this policy. The officers shall use contractual or other appropriate means to protect personal information at a level comparable to this policy while a third party is processing this information.

1.5. Personal information to be collected, retained, or used by the First Filipino Baptist Church Toronto shall be done so only after the officers gives written approval. This information shall be secured according to the officers instructions.

1.6. Any person who believes the First Filipino Baptist Church Toronto uses personal information collected, retained, or used for purposes other than those that the person explicitly approved may contact the officers to register a complaint or to make any related inquiry.

1.7. Upon receiving a complaint from any person regarding the collection, retention, or use of personal information, the officers shall promptly investigate the complaint and notify the person who complained about his/her findings and corrective action taken, if any.

1.8. Upon receiving the response from the officers, the person who filed the complaint may, if he/she is not satisfied, appeal to the First Filipino Baptist Church Toronto Board of Directors to review and determine the disposition of the complaint at issue.

1.9. The determination of the First Filipino Baptist Church Toronto Board of Directors shall be final and the officers shall abide by and implement any of its recommendations.

1.10. The officers shall communicate and explain this policy and give training regarding it to all employees and volunteers who might be in a position to collect, retain, or use personal information.

1.11. The officers shall prepare and disseminate information to the public, which explains the organization's protection of personal information policies and procedures.

## **2. Identifying Purposes**

2.1. The officers shall document the purpose for which personal information is collected to comply with the openness and individual access principles outlines below.

2.2. The officers shall determine the information that will be needed to fulfill the purposes for which the information is to be collected, to comply with the limited collection principle below.

2.3. The officers shall ensure that the purpose is specified at or before the time of collecting the personal information from an individual.

2.4. The officers shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law.

2.5. The officers shall ensure that a person collecting personal information will be able to explain to the individual why this is being done.

2.6. The officers shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is to be collected.

## **3. Consent**

3.1. The officers shall ensure that the individual from whom personal information is collected consents to this and to it being used and disclosed, unless obtaining the consent would be inappropriate.

3.2. The officers shall ensure that the individual can reasonably understand why and how the information will be used when the consent is given.

3.3. The officers shall ensure that no condition is attached to supplying benefits, because of the organization's activities, requiring the individual to give consent for the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

3.4. The officers shall ensure that express consent is obtained whenever possible and appropriate. In rare circumstances, in the officers opinion, having regard to the information's sensitivity and the policy's purpose and intent, implied consent might be acceptable.

3.5. In obtaining consent, the officers shall ensure that the individual's reasonable expectations are respected.

3.6. The officers shall ensure that the express consent obtained from an individual is clear and in an appropriate verifiable form.

3.7. The officers shall ensure that the individual may withdraw consent at any time subject to legal or contractual restrictions and reasonable notice. The individual shall promptly be informed of the withdrawal's implications.

#### **4. Limiting Collection**

4.1. The officers shall ensure that personal information will not be collected indiscriminately. Both the amount and type of information collected shall be limited to that which is necessary to fulfill the purposes identified. The officer shall specify the type of information to be collected, according to the Openness principle.

4.2. The officers shall ensure that information is collected only by fair and lawful means without misleading or deceiving individuals as to the reason.

4.3. The officers shall ensure that the identifying purposes and consent principles are followed in identifying why personal information is to be collected.

#### **5. Limiting Use, Disclosure, and Retention**

5.1. The officers shall ensure that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law, and any use of personal information shall be properly documented.

5.2. The officers shall ensure that all personal information is destroyed, erased, or made anonymous as soon as the purpose for which it was collected is no longer relevant, or as permitted by law. There shall be an automatic review of the need to continue retaining personal information annually. Except as required to be retained by law, all personal information shall be deleted erased or made anonymous no later than seven years after the purpose for which it was collected as been completed.

5.3. The officers shall ensure that all use, disclosure, and retention decisions are made in light of the consent principle, the identifying purposes principle and the individual access principle.

## **6. Accuracy**

6.1. The officers shall reasonably ensure that the personal information is accurate, complete, and up to date, taking into account the individual's interests. The officers shall ensure that the information is sufficiently accurate, complete, and up to date to minimize the possibility that inappropriate information might be used to make a decision about an individual.

6.2. The officers shall ensure that the organization does not routinely update personal information, unless it is necessary to fulfill the purposes for which the information was collected.

6.3. The officers shall ensure that personal information used on an ongoing basis, including information that is disclosed to third parties, shall generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out.

## **7. Safeguards**

7.1. The officers shall ensure that the organization has security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The officers shall do this regardless of the format in which the organization holds the information.

7.2. Depending of the information's sensitivity, the officers may permit reasonable discretion regarding the information that has been collected: the amount, distribution, format, and the method of storage. A higher level of protection shall safeguard more sensitive information according to the consent principle's considerations.

7.3. The officers shall ensure that the protection methods include,

7.3.1. physical measures, for example, locking filing cabinets and restricted access to offices;

7.3.2. organizational measures, for example, security clearance and limiting access on a "need-to-know" basis; and

7.3.3. technological measures, for example, the use of passwords and encryption.

7.4. The officers shall ensure that all employees and volunteers know the importance of keeping personal information confidential, and is to be reviewed with employees and volunteers on an annual basis.

7.5. The officers shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it.

## **8. Openness**

8.1. The officers shall ensure that the organization is open about its policies and practices regarding the management of personal information. The policies and information about the related practices shall be available without unreasonable effort in a form generally understandable.

8.2. The officers shall ensure that the information available shall include,

8.2.1. the name or title and address of the officers who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

8.2.2. the means of gaining access to personal information held by the organization;

8.2.3. a description of the type of personal information held by the organization, including a general account of its use;

8.2.4. a copy of any brochures or other information that explains the organization's policies, standards, or codes; and

8.2.5. what personal information is made available to related organizations.

8.3. The officers shall ensure the information that must be provided according to 8.2 is available either in a brochure at the locations the organization operates, online, or through the mail.

## **9. Individual Access**

9.1. The officers shall ensure that upon request the organization shall inform an individual whether the organization holds personal information about him/her. If possible, the information's source shall also be given. The organization shall allow the individual access to this information. The organization may, however, choose to make sensitive medical information about its employees or volunteers available through a medical practitioner. The organization shall also account for the use that has been made or is being made of this information and give an account as to the third parties to whom it has been disclosed.

9.2. A person requesting his/her personal information may be required by the officers to give sufficient information to permit the organization to provide an account of the existence, use, and disclosure of personal information. Information shall be used only for the purpose for which it was obtained.

9.3. If the organization has supplied personal information about an individual to third parties, the officers shall ensure that an attempt is made to be as specific as possible. When asked to give a list of the organizations to which it has actually disclosed information about an individual is impossible, the organization shall provide a list of organizations to which it might have disclosed information about the individual.

9.4. The officers shall ensure that the organization responds to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be made available in a generally understandable form.

9.5. The officers shall ensure that when an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending on the information challenged, amendment involves the correction, deletion, or addition of information. When appropriate, the amended information shall be transmitted to third parties having access to the information in question.

9.6. The officers shall ensure that when a challenge is not resolved to the individual's satisfaction, the organization shall record the unresolved challenge's substance. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

## **10. Challenging Compliance**

10.1. The officers are authorized to address a challenge concerning compliance with the above principles.

10.2. The officers shall develop procedures to receive and respond to complaints or inquires about the policies and practices regarding the handling of personal information. The compliance procedures shall be easily accessible and simple to use.

10.3. The officers shall inform individuals who inquire about lodging complaints that relevant complaint procedures exist.

10.4. The officers shall investigate all complaints. If a complaint is found to be justified, the officer shall take appropriate measures, including, if necessary, amending the policies and practices.