

SAMPLE POLICY TO PROTECT PERSONAL INFORMATION

1. Accountability

1.1 [name of individual] is hereby appointed as the personal information compliance officer (the "officer").

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 officer.

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 officer 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 Organization shall be done so only after the officer gives written approval. This information shall be secured according to the officer's instructions.

1.6 Any person who believes the organization uses personal information collected, retained, or used for purposes other than those that person explicitly approved may contact the officer 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 officer 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 officer, the person who filed the complaint may, if he/she is not satisfied, appeal to the organization's [board of directors or the trustees] to

review and determine the disposition of the complaint at issue.

1.9 The determination of the [board of directors or the trustees] shall be final and the officer shall abide by and implement any of its recommendation.

1.10 The officer 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 officer 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 officer shall document the purpose for which personal information is collected to comply with the openness and individual access principles outlined below.

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

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

2.6 The officer 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 officer 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. Sometimes personal information can be collected, used, or disclosed without the individual's knowledge and consent. For example, legal, medical, or security reasons might make seeking consent impossible or impractical. When information is being collected to detect and prevent fraud, seeking the individual's consent might defeat collecting the information's purpose. Seeking consent might be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated.

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

3.3 The officer 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 fulfil the explicitly specified and legitimate purposes.

3.4 The officer shall ensure that express consent is obtained wherever possible and appropriate. In rare circumstances where, in the officer's opinion, having regard to the information's sensitivity and the policy's purpose and intent, implied consent might be acceptable. (Implied consent might exist when a church baptizes a new member, and it is generally understood that personal information necessarily obtained in that context will be used for all church-related purposes. Such implied consent should not be

assumed if the church would pass on the personal information to a para-church organization that is not an integral part of the denomination.)

3.5 In obtaining consent, the officer shall ensure that the individual's reasonable expectations are respected. (For example, a person giving his/her name and address to a charity to receive its newsletter or magazine reasonably expects that it will use that information to send other information about itself, But the individual would not likely expect that the information would be used for fundraising.)

3.6 The officer shall ensure that the express consent obtained from an individual is clear and in an appropriately verifiable form. (For example, an application form may be used and kept on file whereon the individual consents to the collection and specific use; a checkoff box may be used to permit information already on file to be used for a new purpose; consent may be given orally which would require the receiver of the consent to create appropriate documentary evidence; or consent might be given by email which would require an electronic record to be maintained.)

3.7 The officer 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 officer 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 fulfil the purposes identified. He/she shall specify the type of information to be collected, according to the Openness principle.

4.2 The officer shall ensure that information is collected only by fair and lawful means without

misleading or deceiving individuals as to the reason.

4.3 The officer 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 officer shall ensure that personal information shall not be used or disclose 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 officer 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 has been completed.

5.3 The officer 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 officer shall reasonably ensure that the personal information is accurate, complete, and up to date, taking into account the individual's interests. He/she 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 officer shall ensure that the organization does not routinely update personal information, unless it is necessary to

fulfil the purposes for which the information was collected.

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

7. Safeguards

7.1 The officer 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. He/she shall do this regardless of the format in which the organization holds the information.

7.2 Depending on the information's sensitivity, the officer 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 officer shall ensure that the protection methods include,

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearance and limiting access on a "need-to-know" basis; and
- (c) technological measures, for example, the use of passwords and encryption.

7.4 The officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential.

7.5 The officer 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 officer 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 officer shall ensure that the information available shall include,

- (a) the name or title and address of the officer who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the organization;
- (c) a description of the type of personal information held by the organization, including a general account of its use;
- (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
- (e) what personal information is made available to related organizations (e.g., organizations that are affiliated).

8.3 The officer 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 officer 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. (Note: If the officer believes for valid reasons that access to personal information should be denied, he/she shall consult legal counsel before making such a decision.)

9.2 A person requesting his/her personal information may be required by the officer 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 officer shall ensure that an attempt is made to be as specific as possible. When 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 officer 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. For example, the organization shall explain abbreviations or codes it uses to record information.

9.5 The officer 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 officer 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 officer is authorized to address a challenge concerning compliance with the above principles.

10.2 The officer shall develop procedures to receive and respond to complaints or inquiries 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 officer shall inform individuals inquiring about lodging complaints that relevant complaint procedures exist.

10.4 The officer 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.