

Privacy Policy - Management of Personal Information			
Source: Standing Committee on Governance	Authority: Standing Committee on Governance	Original Approval Date: 2007 Last Review Date: Nov. 2012	Next Review Date: Nov. 2014
<p>Purpose of Policy:</p> <p>To provide guidelines for the management of personal information (PI) at Eastminster United Church (EUC).</p>			
<p>Theological Rationale:</p> <p>Within the context of its cultural community, the congregation undertakes to honour its legal obligations and statutory requirements, including those related to the collection and management of personal information. As a community of faith, the congregation is resolved to treat its members, adherents and everyone with whom it relates with respect for personhood, dignity and privacy. As a community of believers who would be followers of Jesus, the congregation is committed to developing relationships of mutual support and active caring within its fellowship. Faithfulness requires an appropriate balance between respecting the privacy and personal information of individuals and fostering the openness which is necessary for genuine community.</p>			

1.0 Intent of the Policy

- 1.1 To guard against the inappropriate use of PI at EUC and to safeguard against identity theft.
- 1.2 This policy is consistent with The United Church of Canada’s Personal Information Policy (PIP) and should be read in conjunction with that policy, attached as *Appendix A*.

2.0 Scope of the Policy

- 2.1 This policy encompasses the collection, use, retention, protection, disclosure and disposition of PI for all personal records held at EUC.
- 2.2 It includes a congregational covenant that informs individuals of our pledge to safeguard their PI while in EUC custody. Refer to *Appendix B* for details.

3.0 Definition of Personal Information (PI)

- 3.1 PI includes any factual or subjective information, recorded or not, about an identifiable individual – that is, it is information which can directly or indirectly identify an individual. It does not include the name, title, business address or business telephone number of an employee of an organization.
- 3.2 For a complete description of PI, see *Appendix A*.

4.0 Responsibility for Policy Implementation

- 4.1 The Church Council, through the Governance Committee has the responsibility to oversee this policy.
- 4.2 The Church Council shall appoint a Privacy Official (PO).

- 4.3 The person appointed as PO shall be the Church Administrator. All individuals are to be informed of the name and responsibilities of the PO.
- 4.4 The PO shall be responsible to administer this policy, including the identification, preparation and implementation of appropriate procedures.
- 4.5 The PO shall conduct an annual review of privacy matters to ensure compliance with this policy. Required changes shall be implemented immediately.
- 4.6 The activities of the PO shall be reported to the Church Council regularly and to the congregation annually.

5.0 Guidelines

5.1 The PO shall consider the following guidelines in the management of PI at EUC:

5.2 Collection of Personal Information:

- PI is to be inventoried and assigned the appropriate security level (highly restricted, confidential, and general information) as defined in *Appendix A*.
- The collection of PI for each of these security levels must comply with the UCC PIP guidelines. Procedures must be developed which assure such compliance.
- EUC's website and electronic and paper forms used in the collection of PI shall contain a statement which clearly indicates that such information is protected in compliance with privacy legislation. See *Appendix A* for details.

5.3 Use of Personal Information:

- PI shall only used for the purpose for which it was collected. Information collected shall be the minimum necessary for the identified purpose.
-

5.4 Retention of Personal Information:

- The retention of PI must comply with UCC PIP security levels. Procedures must be developed which assure such compliance.

5.5 Protection of Personal Information:

- PI shall be kept under lock and key and only authorized personnel shall have access to it except in those circumstances when individual access is authorized.
- All necessary precautions should be taken to secure and backup PI that is stored electronically (e.g. up to date anti-virus software, firewalls, password protection, controlled physical access to PI servers and similar methods).
- Regular training is to be provided to staff and volunteers who must be made aware of the importance of maintaining the security and confidentiality of PI. The number of staff and volunteers who are authorized access to PI shall be kept to a minimum.
- Individuals shall be given the opportunity to "opt out" when directories, videos and other types of materials are prepared.
- Third party agents and contractors must comply with federal, provincial and UCC privacy standards. This is to be accomplished through an appropriate provision on contracts and agreements.

5.6 Disclosure of Personal Information:

- The disclosure of PI must comply with UCC PIP security levels and processes must be developed which assure such compliance.
- PI disclosed without consent shall only be done so under those circumstances outlined in the UCC PIP. Essentially this would be in circumstances allowed by law when it is in the best interests of the individual and consent is not readily available. (Details are found in *Appendix A*).

5.7 Disposal of Personal Information:

- PI shall be destroyed once it is no longer required except in cases where federal/provincial retention rules apply.

5.8 Individual Access to Personal Information:

- Individuals shall be provided with controlled access to their own PI. A written request will be necessary.
- Such access must comply with UCC PIP security levels and procedures must be developed which assure such compliance.

6.0 Complaints

6.1 Complaints regarding this policy must be responded to within 30 days. Complaints and responses must be provided in writing.

7.0 United Church of Canada Privacy Bulletins

7.1 Guidelines are issued on an as required basis from The United Church of Canada and forwarded to the Pastoral Charges.

7.2 It is the responsibility of the PO of EUC to ensure these guidelines are implemented

7.3 A list of the current Privacy Bulletins are provided in the table below.

Privacy Bulletin #	Subject	Date Issued
1	Personal Information Protection and Electronic Documents Act (PIPEDA) Frequently Asked Questions <i>(Impact of the Legislation on the United Church of Canada)</i>	March 3, 2004
2	Identity Theft <i>As a responsible partner in an online world, we need to work towards best practices for protecting personal information. This bulletin explores why this is important in The United Church of Canada</i>	September 2004
3	Privacy (Access to Registers) <i>A privacy issue that continues to cause confusion and uncertainty is access to registers. This bulletin provides guidelines when handling these requests and some precautionary steps that should always be followed when access to registers is requested.</i> <i>Sample letters and forms for pastoral charge requests for information in registers.</i>	November 2005