

## APPENDIX 1.5

### **GRACE UNITED CHURCH PRIVACY POLICY**

Reference: UCC Privacy Policy, UCC Privacy Bulletins and FAQ's

Background: The development of a Privacy Policy and Guidelines as well as the appointment of a Privacy Official for Grace United Church is part of a United Church of Canada (UCC) process that started in January 2004 when the federal government passed the Personal Information Protection and Electronic Documents Act (known as PIPEDA). The UCC determined that this act applies to the Church and its pastoral charges and as a result we are obliged to implement its provisions. The UCC head office has appointed a Privacy Officer who is working with a team to try to determine exactly how PIPEDA will impact the UCC and what we should be doing about it. Since 2004 the team has documented their learning in a series of Privacy Bulletins which are available on the UCC website by following the link:  
(<http://www.united-church.ca/en/local/privacy>)

The plan is to eventually roll out a Privacy Program starting at the Conference level, then Presbytery and finally the pastoral charges. While this roll out is being developed (and we expect that it will take some years) the pastoral charges have been asked to develop a preliminary Policy on Personal Information and to appoint a Privacy Official whose duties will include education and auditing.

This policy spells out the responsibility of Grace United Church, its employees and volunteers, regarding the collection, use and disclosure of your personal information in respect to their activities as a not-for-profit organization.

#### KEY HIGHLIGHTS

- Personal information can only be used for the purpose for which it is collected. Specific permission must be sought if personal information is to be used for any other purpose
- Personal information must be stored under lock and key, or on secure computers, and only certain authorized individuals should have access to it
- Once the personal information is no longer required it should be destroyed in accordance with records retention guidelines established by the UCC and with proper authorization
- Pastoral Charges should appoint a Privacy Official who is responsible for the security, integrity, safekeeping and release of personal information

#### DEFINITION

- Personal information includes any factual or subjective information, recorded or not, which can lead directly or indirectly to identification of an individual
- Personal information does not include the name, title, business address or business telephone number or business email, of an employee of an organization
- Personal information will be inventoried, and assigned to one of three levels:
  - Level 1 – Highly Restricted Personal Information – has the potential, through identity theft, of damaging people's lives or their well being and could bring about legal action against the UCC. Examples include compensation employment information such as social insurance number and T4 forms etc, personal medical and health card information, donor name and amount, financial and bank account information, credit card numbers and expiry dates, legal documents that contain personal information, minutes of in camera meetings, disciplinary documentation, organizational restructuring and planning material

Level 2 – Confidential Personal Information – somewhat sensitive and could contribute to identity theft and or legal action against the UCC. Examples include date of birth and date of death, personal email addresses, appointment letters, performance management and reviews, non-medical information related to leaves of absence and disability claims, residential address and phone numbers, complaints, pastoral charge administrative files, compensation information such as salary and benefit amounts

Level 3 – General Information – not sensitive and can be shared. Examples include reference files, periodicals and journals, forms, Council and some committee minutes, Annual Reports, legislation and policies, and published directories

### PRIVACY OFFICIAL

- The United Church of Canada recommends that each congregation appoint a Privacy Official
- A Privacy Official can be anyone designated by the congregation but typically would be someone who is familiar with and has access to most of the information kept on site
- The role of the Privacy Official would be to:
  - Understand and promote the importance and compliance of the Privacy Policy and Guidelines
  - Coordinate the annual personal information audit and maintain related records
  - Work with the owners of the databases in response to requests for personal information at the Conference, Presbytery and/or congregational level
  - Be responsible for the process that allows database owners to ensure security, integrity, safekeeping and release of personal information
- Accountability – the Privacy Official will sit on the Communications Committee and perform his/her duties through the Council/committee structure at Grace

### RESOLVING ISSUES RELATED TO PERSONAL INFORMATION ACCESS

- Generally speaking the individuals should follow the Complaint Resolution Process for Grace United (currently in the adoption process)
- Specifically in regards to Personal Information Access this would (as a minimum) entail:
  - Step 1. The individual and the owner of the database discuss the issue and try to resolve it within the Policy and Guidelines. If there is no resolution then
  - Step 2. The individual and the owner of the database discuss the issue with the Privacy Official, who after reviewing it with appropriate persons within Grace and UCC, will give a recommendation to the parties. If there is still no resolution then
  - Step 3. The parties including the Privacy Official can bring the issue to the Communications Committee who will give a recommendation upon hearing from all the parties. If there is still not resolution then
  - Step 4. The parties may take the issue to Council for final resolution
- As was noted in the background section of this policy we are still at a very early stage in understanding the impact of PIPEDA on the United Church. Therefore it is hoped that any issues regarding Personal Information Access can be addressed in the spirit of dialogue suggested by steps 1 and 2.