Erindale United Church
Privacy Policy

The United Church of Canada (UCC) has a Privacy Standards Policy that allows for the collection, use, management, retention, protection, disclosure and disposition of personal information held at church offices in compliance with all applicable federal and provincial privacy legislation. Erindale United Church will follow this policy.

Principles

Erindale United will follow the ten principles for handling personal information identified in the Personal Information Protection and Electronics Document Act of Canada (PIPEDA).
These principles are: *accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and provision of recourse.*

Personal information will be inventoried, and assigned to one of the three levels:

LEVEL 1 – HIGHLY RESTRICTED PERSONAL INFORMATION

Information is very sensitive and if shared or published inappropriately or harvested electronically for fraudulent activities such as identity theft, has the potential of damaging people's lives and/or their well being and would likely bring about legal action against Erindale United Church.

LEVEL 2 – CONFIDENTIAL PERSONAL INFORMATION

Information is somewhat sensitive and if inappropriately shared, published or harvested electronically could contribute to fraudulent activity such as identity-theft, and bring about hardship or embarrassment to an individual and/or the EUC, or it may bring about legal action against the EUC. The information is used for career development and legislative compliance. This information is considered private, but more individuals have controlled access to it than the information in Level 1.

LEVEL 3 – GENERAL INFORMATION

Information is not sensitive and can be shared. This information is not restricted and many can have access to it. It is collected to assist the departments in the accomplishment of their tasks. There is no confidential or restricted personal information included in this level.

Guidelines

- Personal information can only be used for the purposes for which it is collected. Specific permission must be sought if personal information is to be used for any other purpose than that for which it was initially collected.
- Personal information is to be stored securely (under lock and key and only certain authorized individuals should have access to it.
- To protect against illegal harvesting of personal information, all necessary precautions should be taken to secure and backup personal information that is stored electronically. This should be done with appropriate safeguards that include: up-to-date antivirus software, firewalls, password protection, installation of critical software updates and patches, controlled physical access to personal information servers, and other network security measures.
- Once the personal information is no longer required it should be destroyed except in cases where federal and/or provincial retention rules apply.
- Personal information 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. Personal information does not include the name, title, business address or business telephone number of an employee of an organization. Personal information includes information in any form (eg. printed/electronic) including: home address, home phone-number, age, personal email address, race, national or ethnic origin, colour, religion, sexual orientation, marital status, mental or physical disability, family members' names, employee files, identification numbers, evaluations, disciplinary actions, the existence of a dispute, opinions, comments, social status, income, credit and bank records, donation information, loan records or medical records.
- There has to be a central person who should be knowledgeable about privacy and to whom requests for personal information would be directed. In most cases this person (the *Privacy Official*) is the person who has the most access to the information and who is responsible for the security, integrity and safekeeping of the information.

Implications

- *There should be a clear understanding with members of the congregation on what the council decides how any information can be used, particularly information classified as "General" such as name and address, published phone numbers.*

    - *One option would be to prepare a disclosure to the congregation, with an "opt out" response. To cover uses that a reasonable person might consider, add to the disclosure a clause such as "For administrative purposes, may we share this information with other church committees?"*
        - *Examples for consideration:*
            - *That providing names and phone numbers of members publication and in The Grapevine articles may mean that they are available electronically*

- *Solicitation for Church activities such as :Lectors; Coffee Hosts; Fertilizer Sales.*

- *Council is required to define who is authorized to have access to "Highly Restricted" and "Confidential" information*

- *To demonstrate effective security, there should be a defined process for the record of installation; upgrades and testing of the electronic system security.*

- *There should be a process established and specific records maintained of when information is provided to individuals requesting information contained in church records (Baptisms, Marriages, etc), when it is destroyed, or passed to Archives.*

- *Appoint a Privacy Official*

- *Appoint an individual (or individuals) to be responsible for Erindale United Church's compliance. (Trustees?)*

Appendix 1

Check List of Activities

Analyze all personal information handling practices including ongoing activities and new initiatives, using the following check-list to ensure that they meet fair information practices:

- What personal information do we collect?
- Why do we collect it?
- How do we collect it?
- What do we use it for?
- Where do we keep it?
- How is it secured?
- Who has access to or uses it?
- To whom is it disclosed?
- When is it disposed of?
- Develop and implement policies and procedures to protect personal information:
- Define the purposes of its collection
- Obtain consent
- Limit its collection, use and disclosure
- Ensure information is correct, complete and current
- Ensure adequate security measures
- Develop or update a retention and destruction timetable
- Process to authorize access requests
- Process to respond to inquiries and complaints

Appendix 2

Privacy FAQs

(Compiled from various United Church communications)

Q) We videotape our services for shut-ins. Can we continue this practice given the restrictions of the privacy legislation?

A) If you are videotaping your service for shut-ins using largely wide-angle photography from a distance of a group of people, and for what you consider to be a public event, this should be fine with respect to privacy. If you have members of the congregation who do not want to be photographed, you may want to consider a section of the sanctuary that would not be panned during the taping.

Q) We have individuals walking in off the street and requesting copies of baptismal records. Should we be providing this information?

A) We recommend that you respond to requests for this type of information by asking for:

- a request submitted in writing
- identification if the individual requesting the information is unknown to you

- proof of parenthood if there is any suspicion around the request

Note: You should follow the above practice for any request for personal information.

Q) Is specific permission required to use group or individual pictures on the website?

A) Yes, expressed written consent is required for the posting of photographs, especially those on the Web. The intent is to protect children and youth from unauthorized harvesting of digital photographs from websites by any unscrupulous individuals that may be targeting children.

Q) Is it acceptable, if asked by a member at an annual congregational meeting, to discuss the details of employment expenses?

A) Keeping in mind that this is a matter internal to the church, there are two things to consider:

1. Salary information is considered to be personal information under the Privacy Act.
2. The congregation is the employer and as such it could be argued that members are entitled to know what is being paid to its' employees.

This question has arisen a number of times and as it is an internal matter, and the salary information is not going external to the organization, it should, to our understanding, be left up to the pastoral charge or governing body to determine how they want to handle this information. One suggestion would be to not include this information in the public minutes that are posted on a public website.

Q) Can we share information that we have at the committee level with other committees within the pastoral charge?

A) The Privacy Legislation states that personal information can only be used for the purpose for which it was collected. However, we understand that at times this doesn't seem practical when a duplication of time, effort and information would result. When collecting personal information you may want to consider adding to the form a clause such as "For administrative purposes, may we share this information with other church committees?"

Q) It has been brought to our attention that putting prayer requests in the bulletin may be a violation of the privacy legislation. Can you comment?

A) The Privacy Working Group does not see a problem with putting prayer requests and people's names in the bulletin. In talking to a number of pastoral charges they inform us that they will provide generic types of information-for example, remembering someone who is ill but refraining from divulging specific details.

Q) Do we need to have a Privacy Official at each pastoral charge?

A) Yes, each pastoral charge should have a Privacy Official. There has to be a central person who should be knowledgeable about privacy and to whom requests for personal information would be directed. In most cases the Privacy Official is the person who has the most access to the information and who is responsible for the security, integrity and safekeeping of the information.

Q) We sometimes get requests for forwarding addresses and/or telephone numbers for former ministry personnel. How should we handle these requests?

A) The Privacy Working Group recommends taking the name and telephone number or address of the person making the request and relaying that information to the former minister so that they can contact the individual if they so desire.

Q) Is a person's personal information considered "private" if that information is available through a public resource such as the telephone book?

A) The Privacy legislation allows for the collection, use, and disclosure of personal information that is available through a public resource such as the telephone book. However, keep in mind that some individuals have unlisted telephone numbers and may not want their information used indiscriminately.

Q) **We used to send birthday cards to members on our donor list. Is this a contravention of the legislation?**

A) Age and birthdates are deemed to be personal information, so refrain from sending birthday cards. You may want to consider an alternate generic greeting card letting the recipient know that you are thinking of them or get express written consent for use of personal information for purposes other than that for which it was originally collected.

Q) We used to publish in our bulletin, the names of members of our congregation and addresses of retirement residences and long term care facilities where they reside, so that individuals could send notes and Christmas cards. We are told that we can no longer do this as it is prohibited under the legislation.

A) As we understand it, it is the intent of the privacy legislation to protect individuals from unauthorized use of their personal information and to safeguard personal information from “identity theft”. It is our understanding at this time that the example cited above would not contravene the intent of the legislation. We do, however, urge you to continue to exercise the utmost caution when dealing with personal information.

Q) Are minutes of meetings considered to be personal information?
A) Minutes of a church’s governing body are not confidential. In order to conduct the business of the church court, it may be necessary to move to go “in camera” from time to

time. This should be clearly noted in the minutes, as should any decisions or motions passed in committee of the whole.

Q) Do we have to have a privacy official at each pastoral charge?

A) Yes, someone at each location should be designated the "keeper" of personal information with the information kept in a locked, secure area.

Q) What do I do if I want to access my personal information?

A) A signed, detailed request should be sent to the privacy official at your location or unit.

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

A) No. The church would have to obtain the consent of the member every time the personal information was to be used for different purposes.

Q) The privacy legislation states, "personal information will be retained for only as long as is necessary to fulfill the purpose for which it was collected." Does this affect what records we transfer to our Conference Archives?

A) Archival records are included in the references to legal or business purposes as defined by the Act. Please continue to send your records to your Conference Archives, using the publication *Managing Your Congregation's Records* as a guide.

Q) Congregations frequently take photos/videos of events that are then posted in bulletins, etc. Is consent required by anyone whose photo may be captured and published in the process?

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

Q) Can I refuse to disclose my personal information?

A) An organization, or employer, has the right to obtain your personal information to be able to carry out their day-to-day business, e.g. producing a pay cheque, processing benefits claims, managing donor information etc.