DIOCESE OF EDMONTON

PRIVACY COMMITMENT AND POLICIES

Introduction

Alberta's *Personal Information Protection Act* (PIPA) became law on January 1 2004. PIPA applies in full to the Diocese and all parish corporations.

PIPA requires us to protect the **personal information** of both the public (our church members and those who use our facilities) and our employees. It requires a lot of "reasonableness"—that is, thinking about whether what we do with personal information would make sense to the individual it is about and putting ourselves in that individual's shoes. It establishes rules about collecting, using and disclosing personal information to balance:

- An individual's right to have his or her personal information protected, and
- The diocese and parishes' need to collect, use and disclose personal information for legitimate business purposes.

We must comply with PIPA. As part of this compliance we must commit to protecting personal information. This commitment requires the Diocese and each parish corporation to adopt and enforce policies relating to how we collect, use and disclose personal information.

Commitment to Privacy

The Diocese of Edmonton is committed to protecting the privacy of all individuals who are employed within the diocese, who volunteer their time to the Diocese, members of our congregations and members of those groups who use our church facilities. This policy is designed to inform all of these individuals and groups about our commitment and the practices in place concerning the collection, use and disclosure of personal information provided to the Diocese and parishes, and about the measures that should be in place to protect that information. It applies to all of the activities and undertakings of the Diocese and its parishes; takes effect as of March 1, 2006 and will be reviewed on a regular basis.

Privacy Principles

The following principles constitute a set of Fair Information Practices that will govern how the Diocese will handle personal information. These principles do not replace PIPA and in case of conflict between PIPA and these principles PIPA will prevail. Throughout these principles use of the word **Diocese** includes all parish corporations as well as the diocesan office and all committees established by parishes or the diocese.

1. **Accountability**

The Diocese is responsible for maintaining and protecting personal information that is in its custody or under its control. In order to ensure this, Executive Council will designate an individual or individuals to act as Diocesan Privacy Officer and to be responsible for the Diocese's compliance with these principles and PIPA.

2. Identifying Purposes

Before collecting personal information the Diocese must identify the purpose or purposes for which the information is being collected. We will inform individuals of this purpose on request or when required by PIPA (see section 4 of Guidelines for Collection, Use and Disclosure of Personal Information).

3. **Consent**

An individual's knowledge and consent are required for the collection, use or disclosure of personal information unless PIPA provides for collection, use or disclosure without such consent. Consent may be given in writing, orally or, in certain circumstances may be deemed to have occurred. We will always record when consent is provided (see section 7 of Guidelines for Collection, Use and Disclosure of Personal Information).

4. **Limiting Collection**

The Diocese will only collect personal information that is necessary for the purposes identified by the Diocese. All information must be collected by fair and lawful means and we will not ask for more personal information than is necessary to provide a product or service to an individual. Wherever possible personal information will be collected directly from the individual it is about so that the person is knowledgeable about the purpose of the collection.

5. Limiting Use, Disclosure and Retention

Personal information will only be used or disclosed for the purpose for which it was collected unless an individual has consented to a different use or a disclosure or PIPA permits use or disclosure without consent (see sections 9 & 14 of Guidelines for Collection, Use and Disclosure of Personal Information). Personal information is only retained for the period of time required to fulfill the purpose for which it was collected unless we are required by law to retain for a longer period of time.

6. Accuracy

Every reasonable effort will be made to ensure that we maintain personal information in an accurate and complete form before using it to make a decision, providing a service or disclosing it to another organization.

7. Safeguarding Personal Information

Personal information must be protected by security measures commensurate with the sensitivity of the information. These safeguards are set out in the Diocese's Information Handling and Security Procedures.

8. Openness

The Diocese will provide people with information concerning the policies and procedures that apply to the management of their information. This policy and associated procedures will be available in every parish and at the diocesan office and will be provided at no charge on request. It will also be posted on the diocesan website.

9. Right of Access and Correction

Individuals have the right to be informed of the existence, use and disclosure of their personal information and shall be given access to any personal information about them in accordance with PIPA. The Diocese may charge a reasonable fee for copying personal information. Individuals may verify the accuracy and completeness of their personal information and may request that it be amended to correct any factual error or omission.

10. Handling Complaints and Suggestions

Persons may direct any questions or inquiries with respect to these privacy principles, or about our practices, to the diocesan privacy officer. The name of the diocesan privacy officer and information on how to contact that person will be readily available.

Guidelines for Collection, Use and Disclosure of Personal Information

Personal Information collected before January 1 2004.

1. Personal information collected by the Diocese before January 1 2004 is presumed by PIPA to have been collected with consent. The Diocese will continue to use and disclose it for the purpose for which it was originally collected.

2. If unsure whether the original purpose has been explained to the individuals, define the purpose for which the information will continue to be used and disclosed narrowly and document that purpose in the records.

Collection of Personal Information now.

3. Wherever possible try to collect personal information about an individual directly from that individual.

4. When a person provides personal information voluntarily for a particular purpose, consent to collection for that purpose is implied and no notice of purpose is required. It is good practice to tell people about the purpose of collection at all times.

5. If the information is not provided directly by the individual, written or verbal consent must be obtained from the individual unless PIPA authorizes collection without consent. In such cases, the individual must be informed of the purpose for the collection and consent must be recorded.

6. PIPA does set out some circumstances when collection without consent may occur. Of these, the most frequently used is likely to be:

- When a reasonable person would consider that the collection is clearly in the interests of the individual and consent cannot be obtained in a timely manner or the individual would not reasonably be expected to withhold consent (e.g. getting a phone number to contact a family member in case of illness, emergency or to provide pastoral care; collecting the name of a person for whom prayer is desired; obtaining information about the location of a parish member who is in a hospital.)

Other examples are:

- When collection is pursuant to a statute or regulation that authorizes or requires the collection (e.g. Income Tax Act requires an individual's SIN to issue a T–slip)
- When the collection is from a public body and the public body is authorized to disclose that information to the Diocese (e.g. from Government of Alberta or a registry office)

- When the collection is reasonable for the purposes of an investigation or a legal proceeding (e.g. breach of contract, employee misconduct, defense of a law suit against the Diocese)
- When the collection is necessary to determine the individual's suitability to receive an honour, award or similar benefit, including a scholarship or grant (e.g. financial assistance for attendance at camp)
- When the information is publicly available (e.g. telephone book or other public directory)
- When the information may be disclosed to the Diocese without consent under section 20 of PIPA
- When the collection is necessary in order to collect a debt owed to the Diocese or to enable the Diocese to repay to the individual money owed by it to the individual
- When the information consists only of **personal employee information** that is related to the employment or volunteer work relationship of the individual and, if the individual is an employee of the Diocese, the individual has been provided with reasonable notification that the information is going to be collected and of the purpose for the collection (e.g. employee or volunteer evaluations).

Use of Personal Information.

7. Personal information can only be used for purposes that are reasonable and then only the least amount of information necessary to achieve that purpose should be used. **Use** means when someone authorized by the Diocese accesses the information to carry out a purpose or activity for the Diocese. To determine if a use is "reasonable" ask yourself if the person who provided the information would consider it likely that you would use it for that particular purpose. If not, you need to reconsider using the information for that purpose or obtain consent to use it.

8. Before using or disclosing personal information, you must take reasonable steps to ensure that it is accurate and complete. The Diocese must review lists of personal information such as parish rolls, committee lists and membership lists on a regular basis and keep them up to date. The frequency of review will depend upon the importance of accuracy.

9. PIPA sets out circumstances where you can use personal information without consent. Of these, the most frequently used is likely to be:

- When a reasonable person would consider that the use is clearly in the interests of the individual and consent cannot be obtained in a timely manner or the individual would not reasonably be expected to withhold consent. Some examples of such use are:
    - To contact members of the Diocese or a particular parish (people on a parish roll or diocesan mailing list) about the mission and ministry of the Diocese of Edmonton or that parish. This includes communication about upcoming events, meetings, administrative matters, outreach activities, continuing education and study opportunities, prayer requests and provision of diocesan or parish newsletters.
    - To contact people to participate in or volunteer for ministry activities, including committees, outreach, stewardship, fellowship, liturgical and other ministries.
    - To maintain lists of people who participate in such activities or who have been accredited or recognized in some way (e.g. committee members, synod delegates, persons elected to provincial or general synod, lay readers, and communion assistants).
    - To provide donors to the Diocese with tax receipts.

  Some of the other circumstances where specific consent to use is not required are:
- For the purpose for which consent was given when the information was collected.
- To contact a family member in an emergency situation.
- To respond to an emergency that threatens the health, safety or security of an individual (e.g. a priest is able to use personal information to prevent a threat from being carried out).
- To prepare records for archival appraisal and transfer to an archival institution.
- To recruit or manage personnel and volunteers.

10. If the personal information is publicly available, it may be used for any purpose related to diocesan or parish business. Publicly available information includes personal information in a telephone, professional or business directory, and personal information in a publication or on the Internet if it is reasonable to assume that the individual the information is about supplied the information.

11. An individual who is a member of a parish congregation or a member of a Diocesan committee or board may use personal information contained on the parish roll or register for the purpose of carrying out any authorized activity in the parish or Diocese.

Disclosure of Personal Information.

12. Personal information may only be disclosed for purposes that are reasonable and then only the least amount of information necessary to achieve that purpose should be disclosed. **Disclosure** means showing, telling, sending or giving some other organization or individual the personal information in question. This includes externally to the Diocese (e.g. to Provincial Synod or Church House) and within the Diocese when the information passes from one area to another for a purpose unrelated to why it was collected (e.g. from one committee or board to another unrelated committee or board).

13. When asked by an external organization for personal information, ask the individual making the request why the information is needed and what their authority is to collect it. If in any doubt as to whether disclosure is authorized, seek advice from the Privacy Officer (or legal advice) as to whether you can make the disclosure without consent, or seek the consent of the individual concerned before making the disclosure. You may also offer to provide the name and contact information of the requestor to the individual concerned.

14. Some circumstances when disclosure may take place without consent are:
    - When a reasonable person would consider that the use is clearly in the interests of the individual and consent cannot be obtained in a timely manner or the individual would not reasonably be expected to withhold (e.g. providing a name and telephone number to contact a family member in the case of an emergency, including a pastoral emergency; placing a person on a prayer list).
    - When the personal information is disclosed to a public body that is authorized to collect the information under an enactment (e.g. a report of an injury to the Workers' Compensation Board; disclosure of financial donations to Canadian Customs and Revenue Agency for an investigation; disclosure to the Alberta Human Rights Commission).
    - When the disclosure is necessary to comply with a subpoena, warrant or court order.
    - When a public body or police service needs help in an investigation from which a law enforcement proceeding is likely (e.g. police investigation of a robbery or assault).
    - If the disclosure is reasonable for the purposes of an investigation or legal proceeding (e.g. to legal counsel for the Diocese or for an internal investigation under the Canons of the Diocese).
    - When the information is disclosed to respond to an emergency that threatens the health or safety of an individual or the public (e.g. someone threatens to harm another person or himself and disclosure can prevent or reduce the chance of the threat being carried out).
    - When the next of kin or friend of an injured, ill or deceased individual needs to be contacted.
    - When collecting a debt owed to the Diocese or a parish (e.g. to a collection agency or to someone who may know the location of the debtor).

- When the information is publicly available as described in 10 above.
- To the surviving spouse, adult partner or relative of a deceased individual (e.g. circumstances surrounding the death or information provided to a priest or lay person and intended for the spouse, partner or relative).
- To determine if the individual is suitable for an honour, award or other similar benefit, including financial assistance (e.g. to provide background information about an individual for a scholarship).
- To an archival institution for the preservation of church records.
- To an individual who has signed an agreement for access to the information for research purposes.
- When the information is **personal employee information,** the individual is or was an employee or the information is being collected in order to decide whether to hire a potential employee (e.g. references).

Information Handling and Security Procedures

The Diocese will use reasonable safeguards to protect personal information from such actions as:

- Someone getting access to, or collecting, copying, using or disclosing personal information when he or she is not supposed to;
- Someone misusing, stealing or losing personal information;
- Someone who is unauthorized to do so collecting, using, disclosing, copying, changing or destroying personal information;
- Not destroying or disposing of personal information in a secure manner.

Where a parish does not have the resources to comply with these procedures in their entirety, it must make its best efforts within its resource constraints to protect personal information and comply with these procedures to the extent possible.

ADMINISTRATIVE SAFEGUARDS

1. The Diocese will ensure that the Diocesan Privacy Policy and Guidelines are made available to all staff and volunteers. When hiring new staff or recruiting volunteers who will have access to personal information, these staff and volunteers shall read the Privacy Policy and Guidelines and have the opportunity to ask questions about how they apply to their work.
2. **Employees** will be trained to know the rules for protection of personal information.
3. Employees will sign an oath of confidentiality if they are users of personal information on a regular basis.
4. An employee will be assigned in each parish and at the Diocesan Office to be systems administrator, or a contract will be signed with a computer company to perform these duties.
5. The least amount of personal information necessary for the intended purpose will be used or disclosed and only to employees who have a need to know that information.
6. Reasonable steps will be taken so that personal information transmitted verbally cannot be overheard or intercepted. This includes the use of private offices or rooms when discussing sensitive personal information.
7. Employees shall report any violations or suspected breach of privacy or information security as soon as possible to the Diocesan Privacy Officer so that corrective action can be taken to resolve the immediate situation and minimize the risk of further occurrences.

PHYSICAL SAFEGUARDS

1. All paper and electronic records will be held and stored in an organized, safe and secure manner. Areas where personal information is stored shall be equipped with fire detection and suppression devices (e.g. smoke detectors, fire extinguishers, sprinkler systems) that are checked on a regular basis for safety.

2. Parishes will designate someone to exercise control over keys that provide access to areas where personal information is stored or used. Only employees who have signed a confidentiality oath should have keys to these areas.
3. Personal information will not be left displayed or unattended in public areas.
4. Personal information will be stored in locked cabinets or desks, or in locked rooms, when not in use.
5. Servers or other computers that house personal information will be kept in a locked room, locked cabinet or will be secured to some permanent fixture to reduce the risk of theft.
6. Personal information will be shredded and not placed in a garbage can or recycling container. Documents waiting to be shredded should be boxed and placed in a locked room.
7. Any personal information being transported or left for pick up will be in a sealed envelope addressed to the person for whom the information is intended and marked 'confidential'.
8. All fax transmissions containing personal information will be sent with a cover sheet. The cover sheet will include a notification that the information is confidential and intended only for the named recipient and asking that if the fax is received in error the person receiving the fax telephone the sender immediately and not make any copy. Employees should double check fax numbers for accuracy before sending personal information and if using preprogrammed numbers these numbers should be re-verified twice a year.
9. Prior to disposal of electronic storage media (e.g. disks, CDs, tapes or hard drives) the media will be destroyed so as to be unusable.
10. Servers or computers housing personal information will be protected from power surges or power outages by a surge protector and UPS battery. The UPS battery should be checked monthly and replaced if needed.
11. Any laptop computers, tablets or personal digital assistants (PDAs) that contain personal information shall be kept secure. They must always be locked up and out of sight if left in a vehicle or are out of the possession of the user.

TECHNICAL SAFEGUARDS

1. Information systems users shall be assigned a unique User ID and password for the systems. The User ID shall restrict access to data and systems containing personal information to that required by the user for their duties to the Diocese or parish.
2. Passwords are to be kept confidential at all times and should not be shared with others or written down except for security purposes.
3. Systems containing personal information shall be backed up daily and the back up media stored off site in a secure place. There will always be one copy of back up data off site and that copy shall not be older than 1 week. The employee responsible for back up will check to ensure that the back up was successful each day and will ensure that the back up media is capable of restoring data by performing restoration tests at least twice a year.
4. All computers housing personal information and connected to the Internet shall have antivirus protection installed that is updated automatically. An employee shall be

designated to ensure that the subscription for the antivirus protection is renewed as required.

5. A firewall must be in place to protect computers from malicious interference. When possible a hardware firewall should be used, but software firewalls are permitted.
6. An employee or contracted system maintenance company shall ensure that all software updates, security updates and patches to the operating system are properly installed and that regular system maintenance is performed on a monthly basis.
7. Personal use of the Internet is discouraged and downloading of music, screensavers and other programs that could damage or interfere with personal information is prohibited.
8. Personal information will not be sent by electronic mail unless encrypted or in a password protected attachment to the e-mail message. The password should be communicated by telephone or in person.
9. If laptops or tablets are used in a wireless network, precautions will be taken to ensure that factory settings are disabled and that the wireless network is secured through encryption against outside use or interception of personal information.
10. If a computer is used by several employees and access restrictions are impractical, sensitive personal information such as donation records, employee information or pastoral information must be stored on removable media and kept in a locked container when not in use.

HOME OFFICES

If personal information that is in the custody or control of the Diocese is taken home, it is the individual's responsibility to take reasonable steps to protect that information. This includes:

- Ensuring that records are secure in the home and not left where they are visible or accessible to family members or visitors
- Ensuring that any Diocesan information is protected on a home computer or portable computing device by such means as passwords or partitioned drives.
- Ensuring that records are secure during transportation and are not left where they are visible or accessible to others in a vehicle.
- Returning records to the Diocese as soon as practicable after home use.

Definitions and Interpretation

Diocesan means of or belonging to the Diocese of Edmonton or a parish.

Diocese means the Diocese of Edmonton and all the parish corporations within the diocese.

Employee means an individual who is employed by the Diocese; an individual who performs a service for, in relation to or in connection with the Diocese as a volunteer, participant or student' and an individual who performs a service under a contract or agency relationship with the Diocese.

Firewall means a hardware or software device that restricts external access to a computer or network. Firewalls may be on a router or be software loaded on to a computer. Firewalls must be activated to be operational.

Password is the unique identifier created by an individual to authenticate that the individual is using the computer or computer program. Passwords should be 6 – 8 characters in length and include numerals or symbols.

Personal Employee Information means personal information reasonably required by the Diocese that is collected, used or disclosed solely for the purposes of establishing, managing or terminating and employment relationship or volunteer relationship between the Diocese and the individual. It applies to personal information about existing and potential employees or volunteers. It does not include personal information about an individual that is not related to the employment relationship.

Personal Information means information about an identifiable individual. PIPA does not apply to non-identifying information (e.g. statistical information or aggregate information) or to information about diocesan or parish administration or activities.

PIPA means the Personal Information Protection Act and the Personal Information Protection Act Regulation, as amended from time to time. The Regulation contains further definition of what is "publicly available" and sets out guidelines for archival material.

Portable Computing Device means a laptop, tablet or personal digital assistant (such as a Blackberry or Palm Pilot) on which personal information may be stored.

Reasonable means what a reasonable person would consider to be reasonable in the circumstances.

Right of Access means the right of an individual to view or have copies of his or her personal information.

Systems Administrator means the individual who is responsible for day to day maintenance or a computer or computer network, including assigning user rights to employees, ensuring updating of operating systems and security systems, ensuring protection against viruses and backing up data.

UPS means an uninterruptible power supply that will provide sufficient power to enable orderly shut down of the computer or computer network.

User ID means the unique identifier assigned to each computer user.