Procedures & Guidelines

Governing the collection, management, retention and disposition of personal information held by the Diocese

Privacy Standards Policy

Jesus teaches us the dignity and worth of every human being. In our baptismal covenant, we promise to follow that teaching faithfully: *Will you strive for justice and peace among all people, and respect the dignity of every human being? I will, with God's help.*

In accord with this covenant, the Anglican Diocese of Ottawa has approved a Privacy Standards Policy and associated procedures and guidelines covering the collection, management, retention and disposition of personal information held by the Diocese. Also useful is a checklist to help parishes and agencies assess their own handling of personal information, and a summary of "Do and Don't" with respect to website privacy.

- Privacy Standards Policy, updated 2011
- Check list for parishes and agencies
- Web and publication privacy Do's and Don't

Any questions on the policy, procedures, guidelines or complaints received about the handling of personal information held in a diocesan office, agency or parish should be directed to the Diocese Privacy Officer.

Overview

Purpose of the Policy

The Privacy Standards Policy and related procedures and guidelines are intended to ensure the proper collection, retention and distribution of personal information by the Diocese of Ottawa, its agencies and its parishes, to reflect the federal *Personal Information Protection and Electronics Document Act* (SC 2000 c. 5). The Policy and the procedures and guidelines are to be followed by all individuals, lay or ordained, paid or unpaid, who serve the Diocese under the jurisdiction of the Bishop of Ottawa or in the parishes which make up the Diocese.

Definition of personal information

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. Personal information includes information in any form, such as: home address and home phone number, age, marital status, family members' names, photographs or digital images of a person, employee files, identification numbers, ethnic origin, evaluations, disciplinary actions, the existence of a dispute, opinions, comments, social status, income, credit records, donation information, loan records or medical records.

Personal information does **not** include the name, title or business address or business telephone number of an employee or volunteer of an organization.

Principles upheld

The Diocese follows the ten principles for handling personal information as set out in Schedule 1 to the *Personal Information Protection and Electronics Document Act* (SC 2000 c. 5). These principles are: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and provision of recourse. See the Policy for more detail.

All personal information is the property of the Diocese of Ottawa and all individuals have controlled access to their personal information. All personal information obtained by other organizations or agencies on behalf of the Diocese must be handled in compliance with standards comparable to the Diocese Privacy Standards Policy. This includes the signing of the diocese confidentiality agreement and provisions in the contract of work regarding the protection of the personal information.

Consent

In general, persons must be advised of the purpose for which their personal information is being collected, and how and when it will be used or disclosed. Then they must consent to its retention in diocesan records.

There are some exceptions to this principle.

The Diocese may collect and use personal information without consent

(a) if it is clearly in the individual's interest and consent is not available in a timely way
(b) if collection is required to investigate the breach of an agreement or the contravention of a federal or provincial law
(c) for journalistic, artistic or literary purposes
(d) if it is publicly available
(e) for an emergency that threatens an individual's life, health or security, or
(f) for statistical or scholarly study or research.

In addition, the Diocese may disclose personal information without consent

(a) to a lawyer representing the Diocese
(b) to collect a debt the individual owes the Diocese
(c) to comply with a subpoena, warrant or order made by a court or other juridical body
(d) to a lawfully authorized government authority
(e) in the case of an emergency that threatens an individual's life, health or security
(f) when the information was recorded more than 100 years before the proposed time of disclosure or is to be disclosed more than 20 years after the person's death.

Where information is retained

The Diocese has a centralized record management process for the collection, management, retention and disposition of personal information.

Information about clergy, employees and many volunteers is located the Diocese office. Each clerical and staff member of the Diocese, whether full-time, part-time or contract, has

a confidential and secure personnel file located in the Diocesan office. Congregational information is contained in parish files in the Administration and Finance Office and is stored in locked file cabinets. The Administration and Finance Office manages donor record information.

Parishes retain information on staff, on the congregational membership, on pastoral care matters and on the financial and organizational aspects of parish operations.

Application of Policy and procedures

Each office, agency or parish is responsible for following procedures for collection, retention and distribution that are in accordance with the Policy and related procedures and guidelines. The Privacy Standards Policy and these procedures and guidelines will be made available to Diocese staff. Employees will be made aware of the importance of maintaining the security and confidentiality of personal information. The misuse or improper handling of personal information may result in disciplinary action up to and including dismissal.

Privacy Officer

The Bishop of the Diocese has appointed a Privacy Officer for the Diocese of Ottawa with responsibility to ensure compliance with the Diocese's Privacy Standards Policy. Diocese staff and parishes will be informed of the name and responsibilities of the Privacy Officer.

Responsibilities

1. The Privacy Officer reports to the Bishop and Diocesan Council on a regular basis with regard to any activities related to personal information protection.

2. The Privacy Officer co-ordinates the response to any complaints made to the Diocese, one of its agencies or its parishes regarding the handling of personal information held about that person.

3. The Privacy Officer will investigate any handling of personal information which is inconsistent with this Policy.

4. The Privacy Officer will ensure regular training for staff/volunteers of the Diocese with respect to the policies and procedures required to protect personal information and will provide advice to privacy contacts and others as required.

5. The Privacy Officer, in consultation with privacy contacts, will review periodically the Diocese Privacy Standards Policy and will propose amendments to the Policy, as required, to the Bishop and Diocesan Council.

6. The Privacy Officer will have a copy of the approved Privacy Standards Policy and the associated procedures and guidelines placed in staff reference materials and on the Diocese website.

Privacy Contact

Each office, agency and parish of the Diocese will assign at least one person to be their Privacy Contact. Privacy Contacts are responsible for coordinating the application of the Privacy Standards Policy and associated procedures and guidelines within their office, agency or parish, and to receive any queries on privacy matters from the Privacy Officer or others.

Access, enquiries and complaints

In all cases, care should be taken to confirm that the person making the enquiry or complaint or otherwise seeking access to personal information is the person about whom personal information is held or is a person entitled in law to have access to such information. In any case of doubt, the matter should be referred to the Privacy Officer.

Access

1. All requests for personal access to records held about that individual will be made in writing.

2. A request for access shall be responded to within a reasonable period, not later than 30 days of receipt.

3. Persons about whom the Diocese holds personal information may access those records in the presence of the office, agency or parish Privacy Contact or other official designated by the head of the office, agency or parish.

4. Access to certain parts of her/his personal records by that person may be denied if:
   a) that information is protected by solicitor-client privilege
   b) access could reasonably be expected to threaten the life or security of another individual
   c) that information was generated in the course of a formal dispute process
   d) the individual's knowledge of the information collection would compromise an investigation of a breach of an agreement or the contravention of the laws of Canada or a province
   e) access would reveal confidential commercial information
   f) access would give that person access to personal information about another person.

5. Where access to certain information is to be denied for one of the reasons described above, but part of the record need not be denied and can be severed from the confidential part of the record, access to that portion may be granted.

6. In a case where denial of access to all or part of a record of personal information is contemplated, the office, agency or parish must coordinate that denial with the Privacy Officer.

Enquiries

1. Enquiries regarding personal information held by the Diocese, or one of its offices, agencies or parishes shall be referred to the relevant Privacy Contact for response.

2. A response to such an enquiry should be made within a reasonable period.

3. The Privacy Contact may consult the Privacy Officer on the Diocese Policy regarding the handling and disclosure of personal information for purposes of responding to the enquiry.

Complaints

1. Complaints about the handling of personal information held in diocesan offices, agencies or parishes shall be referred to the Privacy Officer immediately on receipt.

2. The Privacy Officer will coordinate the response to the complaint with the relevant Privacy Contact(s).

3. The person making the complaint will be advised, immediately following its receipt, that it has been referred to the Privacy Officer, along with the Officer's name and contact information. Where the complaint has been received in writing, the advice should be in writing.

When the policy is not followed

If a Diocese office, agency or parish gathers, uses or discloses personal information in a manner inconsistent with the Diocese Privacy Standards Policy, the Privacy Officer will investigate and prepare a report. A copy of the report will be provided to the office, agency or parish.

If the investigation indicates that the gathering, use or disclosure was inadvertently inconsistent with the Privacy Standards Policy, the Privacy Officer and head of the office, agency or parish will review the office, agency or parish's procedures including staff training, and will undertake any corrective measures necessary.

If the office, agency or parish gathered, used or disclosed personal information in a manner it knew was inconsistent with the Diocese Privacy Policy, the Privacy Officer will provide a copy of the report on the matter to the Bishop's Office for such action as the Bishop or his/her delegate directs.

Any questions on the Policy or these procedures and the following guidelines, and any complaints received about the handling of personal information held in a diocesan office, agency or parish should be directed to the Privacy Officer.

Privacy Officer (613) 232-7124, Ext. 255

Guidelines

Information identification and classification

Each office, agency and parish will follow procedures for collection, retention and distribution that reflect the Privacy Standards Policy, the procedures and the guidelines described below.

The first step is to classify incoming personal information and thereby determine how it is to be handled. There are three standard levels of security:

Level 1 – Highly Restricted
Level 2 – Confidential
Level 3 – General Information

The type of information collected, consent required, retention period and disposition will vary with each level.

Level 1 – Highly Restricted

Criteria	Information is very sensitive and if shared inappropriately has the potential of damaging people's lives and/or their well being and could bring about legal action against the Diocese. The information is used for internal judicial decisions, identifies donor designations, career development, compensation determination, and legal action.
Examples	▪ Personal medical information ▪ Donor name and amount, financial and bank information ▪ Legal documents that contain personal information ▪ Disciplinary documentation or sexual misconduct complaints ▪ Organizational restructuring and planning material ▪ Compensation information such as social insurance number, job ranking amounts ▪ Personal information gathered as part of pastoral duties ▪ Medical records
Collection	1. Collect personal information only for a specific purpose and limit the amount and type of information gathered to what is necessary for the identified purposes. 2. Advise the individual of the purposes for which information will be used or disclosed, at or before the time of information collection. This may be done orally or in writing. If consent is granted or denied orally, then a follow-up letter must be issued to confirm in writing that the office, agency or parish's records reflect the individual's wishes. A copy of the letter is to be kept on file. 3. Consent must be obtained again when collected information might be used for another purpose. 4. Personal information, stored electronically, is not to be downloaded without the written consent of the head of the office, agency or parish, who also reports this access to the Privacy Officer.
Retention	1. Keep personal information only as long as is necessary to satisfy the purposes for which it was collected, but a) information associated with compensation, disciplinary, legal and judicatory decisions is to be retained for an indefinite period of time, and b) donor, restructuring, medical and job evaluation information is destroyed as soon as it is no longer necessary. 2. To safeguard from unauthorized access, disclosure, copying, use or modification, information must: a) be kept in a locked file cabinet separated from the general personal files, if it will be used for disciplinary, juridical or misconduct information b) be accessed only by officers listed on an access list, c) be password protected by using security software and passwords where the data is in electronic format; d) be accessed only by those who "need to know"; e) be placed in the Archives, sealed and stamped with a date and a list of those who have access, when files with personal information related to disciplinary, juridical or misconduct activities are no longer active. 3. Destroy, erase or render anonymous information that is no longer required for an identified purpose or legal requirement. 4. Dispose of personal information in a manner that prevents improper access. Shredding paper files or deleting electronic records are recommended. Any electronic equipment no longer used will be reformatted to ensure all personal information is over-written; simple deletion of files from the computer will not accomplish this.
Distribution and individual access	1. Information is restricted to very few individuals/positions placed on a predetermined list. 2. Information must only be disclosed for the purpose it was collected. 3. Distribute personal information in a manner that prevents improper access. 4. Individuals have controlled access to their own personnel files and any other personal information collected about them, except for the consent exemptions listed above. 5. All points above apply to both written and electronic information.

Level 2 – Confidential

Criteria	Information is somewhat sensitive and if shared inappropriately could bring about embarrassment to an individual and/or the Diocese or cause legal action against the Diocese. The information at this level is used for career development and legislative compliance. It is considered private, but more individuals have access to it then the information in Level 1.
Examples	▪ Appointment letters ▪ Performance management and reviews ▪ Leaves of absence and disability ▪ Residential address and phone numbers ▪ Photographs or digital images of a person* ▪ General complaints ▪ Parish files ▪ Compensation information such as salary and benefit amounts *Photographs and digital images of children *Consent for the collection, retention and use of the images of children must be obtained from the child's legal guardian.*
Collection	1. Collect personal information only for a specific purpose and limit the amount and type of information gathered to what is necessary for the identified purposes. 2. Advise the individual of the purposes for which information will be used or disclosed, at or before the time of information collection. This may be done orally or in writing. If consent is granted or denied orally, then a follow-up letter must be issued to confirm in writing that the Department's records reflect the individual's wishes. A copy of the letter will be kept on file. 3. Consent must also be obtained again when collected information might be used for another purpose. 4. Personal information, stored electronically, will not be downloaded electronically without the written consent of the head of the Office, agency or parish, who reports this access to the Privacy Officer.
Retention	1. Keep personal information only as long as is necessary to satisfy the purposes a) Information is to be retained for a definite period of time (7 years or as otherwise designated by the Office, agency or parish). b) All information is destroyed as soon as it is no longer necessary 2. To safeguard from unauthorized access, disclosure, copying, use or modification information must: a) be kept in a locked file cabinet b) be accessed by officers listed on an access list, c) be password protected by using security software and passwords where the data is in electronic format. d) be accessed only by those who "need to know" 3. Destroy, erase or render anonymous information that is no longer required for an identified purpose or legal requirement. 4. Dispose of personal information in a manner that prevents improper access. Shredding paper files or deleting electronic records are recommended. Any electronic equipment no longer used will be reformatted to ensure all personal information is over-written; simple deletion of files from the computer will not accomplish this.
Distribution and individual access	1. Information is restricted to individuals/positions on a predetermined access list. 2. Information must only be disclosed for the purpose it was collected. 3. Distribute personal information in a manner that prevents improper access. 4. All points above apply to written and electronic information. 5. Individuals have controlled access to their own personnel files and any other personal information collected about them, except for the consent exemptions listed above. 6.

Level 3 – General Information

Criteria	Information at this level is not sensitive and can be shared. It is not restricted and many can have access to it. It is collected to assist the diocesan offices, agencies, or parishes in the accomplishment of their tasks. There is no confidential or restricted personal information included in this level.
Examples	▪ Reference files ▪ Periodicals and Journals ▪ Forms ▪ Board and Committee minutes (see below) ▪ Annual Reports ▪ Legislation and policies
Collection	Personal information is not to be collected in this category.
Retention	1. Keep information only as long as is necessary to satisfy the purposes 2. Safeguard from unauthorized access to ensure information is not modified or lost.
Distribution and individual access	Information can be shared publicly.