Diocesan Centre Privacy Standards Policy

Diocese of Toronto
Anglican Church of Canada

Purpose

The Diocese of Toronto has a Privacy Standards Policy, applicable to all individuals, lay or ordained, paid or unpaid, who serve in the Diocesan Centre under the jurisdiction of the Bishop of Toronto, to ensure the proper collection, retention and distribution of personal information.

Collection

The Diocesan Centre 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 on the central database of the Diocesan Centre. Each cleric and employee of the Diocese, whether full-time, part-time or contract, has a confidential and secure personnel file located in the Records Office. Congregational information is contained in parish files in the Records Office and is stored on the central database of the Diocesan Centre. The Stewardship Development Office manages all donor record information. All personal information is the property of the Incorporated Synod of the Diocese of Toronto and all individuals have controlled access to their personal information. All Diocesan Centre personal information obtained by other organisations and agencies must comply with standards comparable to the Diocesan Centre Privacy Standards Policy.

Definition

Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. Personal information does not include the name, title or business address or telephone number of an employee of an organisation. Personal information includes information in any form, such as: home address and home phone number, age, marital status, family members' names, 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.

Principles

The Diocesan Centre will follow the ten principles for handling personal information as set out in Schedule 1 to the Personal Information Protection and Electronics Document Act of Canada.. These principles are: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and provision of recourse.

Accountability

The Diocesan Bishop, after consultation with the Bishops and Directors, will designate a person to be the Privacy Officer in the Diocesan Centre Office with responsibility to ensure compliance with

the Diocesan Centre Privacy Standards Policy. Staff must be informed of the name and responsibilities of the Privacy Officer. The Privacy Officer will report to the Diocesan Bishop for discussion on a regular basis in regard to any activities related to personal information protection. The Privacy Officer will ensure regular training for staff/volunteers as to the policies and procedures personal information protection requires. The Policy will be reviewed periodically by the Privacy Officer, in consultation with the Department Privacy Contacts, and placed in the Diocesan Staff Manual. 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.

Each department will assign one person responsible for ensuring the standards are maintained. Each department must follow the procedures for collection, retention and distribution listed below and assign personal information to one of the three levels:

Level 1 – Highly Restricted

Level 2 – Confidential

Level 3 – General Information

Exceptions to the Consent principles:

The Diocesan Centre may collect and use personal information without consent:

a. If it is clearly in the individual's interests and consent is not available in a timely way

b. If collection is required to investigate a breach of an agreement or 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

f. For statistical or scholarly study or research.

The Diocesan Centre 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

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
- College of Bishops' Minutes
- Disciplinary documentation
- Organizational restructuring and planning material
- Compensation information such as social insurance number, job ranking amounts

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 without the written consent of the Director of the Department who reports this access to the Bishops and Directors and the Privacy Officer.

Retention

1. Keep personal information only as long as is necessary to satisfy the purposes

    a. Information associated with compensation, legal and judicatory decisions are to be retained for an indefinite period of time

    b. Donor, disciplinary, 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, will be used for disciplinary, juridical or misconduct information

    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. Approval of security software must be received by the Manager of Office Services, and reported to the Privacy Officer.

    d. be accessed only by those who "need to know"

    e. be placed in the Records Office, sealed and stamped with a date and a list of those who have access, when the personal information is related to disciplinary, juridical or misconduct activities

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 ideal. Any electronic equipment no longer used will be formatted to ensure all personal information is over-written.

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 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 it may bring about legal action against the diocese. The information is used for career development and legislative compliance. This information 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
- Complaints
- Parish files
- Compensation information such as salary and benefit amounts

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 Director of the Department who reports this access to the Bishops and Directors and 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 department)

    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. Approval of security software must be received by the Manager of Office Services, and reported to the Privacy Officer.

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 ideal. Any electronic equipment no longer used will be formatted to ensure all personal information is over-written.

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 access to their own personnel files and any other personal information collected about them, except for the consent exemptions listed above.

Level 3 – General Information

Criteria

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.

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

Keep information only as long as is necessary to satisfy the purposes

Safeguard from unauthorized access to ensure information is not modified or lost.

Distribution and Individual Access

1. Information can be shared publicly.

2. All major Board and Committee minutes produced after May 16th, 2002 can be shared publicly. All major Board and Committee minutes produced before May 16, 2002 will be screened to remove personal information before any public distribution.