Diocese of Huron

The Anglican Church of Canada

Confidentiality and Privacy Standards Policy

Revised (April 2, 2004)

The Diocese of Huron is committed to providing ministry to all persons. In order to provide a secure and confidential environment in which we can proclaim the Gospel of Christ with integrity and respect, it is necessary to take measures that will provide a level of confidentiality and privacy to all those who seek our ministry and for those who do ministry.

To this end, one of the policies in place is the Diocese of Huron Privacy Standards Policy which takes into consideration that in order to do ministry and in order to comply with various Government regulation relating to maintaining records on employees, etc., the policy allows for the collection, management, retention and disposition of personal information held at Huron Church House (190 Queens Ave., London) and at the Verschoyle Philip Cronyn Memorial Archvie (1349 Western Road, London). The complete Policy is reproduced here. Any questions on the policy should be directed to the Interim Privacy Officer.

Privacy Standards Policy

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

Collection:
Huron Church House 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 electronically on a central database at Huron Church House. Each cleric and employee of the Diocese, whether full-time, part-time or contract, has a confidential and secure personnel file located in the Human Resources Department as well as in payroll files in the payroll office. A payroll service is utilized to administer payroll for parish and Diocesan staff. Congregational information is secured in parish files in several departments and is stored electronically on the central database at Huron Church House. The Development Office and Accounting Department manages all donor record information. All personal information is the property of the Incorporated Synod of the Diocese of Huron and all individuals have controlled access to their

personal information. All personal information obtained by other organizations and agencies must comply with standards comparable to the Diocesan Privacy Standards Policy (i.e. payroll administration, benefits providers).

Definition:
Personal information includes any factual or subjective information, recorded or not, about an individual. Personal information does not include the name, title or business address or telephone number of an employee of an organization. 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:
Huron Church House staff will follow the ten principles for handling personal information as set out in Schedule 1 of 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 will designate a person to be the Privacy Officer in the Diocese with responsibility to ensure compliance with the Diocesan 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 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.

All staff at Huron Church House are required to sign a confidentiality and privacy statement and failure to comply with the Diocesan Confidentiality Policy will be grounds for 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:

Huron Church House 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.

Huron Church House 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
- Deployment/Hiring actions
- 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 Director, Administration and Finance, and reported to the Privacy Officer.
   (d) be accessed only by those who "need to know"
   (e) be placed in the Bishops 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.

5. 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
- Certain financial records and annual reports
- Annual Reports and Statistics
- Synod Journal and Reports

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 Director, Administration and Finance, 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:

- Periodicals and Journals
- Forms
- Committee Minutes and Parish Board Minutes
- 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

1. Information can be shared publicly.
2. All major Board and Committee minutes will be screened to remove personal information before any public distribution.

Access to Personnel Files:

Employees and seminary students may review the contents of their personnel records by contacting the Privacy Officer and making an appointment to review their file.

PARISH RESPONSIBILITIES

Parishes should review the above policy in relation to information which they are collecting or may wish to collect in the parishes for use. The following should be considered in regards to all information they are collecting or currently have in their possession.

1. What information are they collecting and for what purpose?

2. Who will have access to the information?

3. Who are they releasing that information to? Congregations should consider such information such as parish registries, parish lists, donation records, etc.

4. Ensure that they have signed consent from those who are having their photographs taken for the photo directory and that those people are allowing their names, addresses, and phone numbers to be printed in the directory. Parishes should consider to

whom the directory is being distributed. If advertising is sold in the directory, the parish should consider signed consent before distributing the directory to non-members of the church.

5. Ensure they use the information and lists only for the purpose that they have received consent from the member of the congregation providing that information. All police record checks which are requested for the purposes of Screening In Faith should be seen by the Screening In Faith Officer or the rector of the parish and in the file it should be noted that the person's Police Records Check has been reviewed and it should be returned to the person to whom it belongs. Parishioners who need to have documents such as parish lists in their personal possession should be required to sign confidentiality statements. The signing of confidentiality statements are recommended for all who are in ministry roles in the which they have access to confidential or personal information (positions such as Pastoral Care Visitors, Lay Eucharist Minister, etc.).

6. Parishes should ensure that information that is being released such as copies of baptismal information, weddings and confirmations is being released to people who are entitled to receive that information.

7. Parishes should add a privacy disclaimer to their personal website.

8. Parishes should add a Privacy Signatory at the end of emails and faxes. Sample phrases include: PRIVACY POLICY: This email message is confidential, for the exclusive use of the addressee. If you are not the intended recipient of this message, please delete this information.

9. In regards to personal information being requested from the parish over the telephone such as telephone numbers of members of the congregation, the person inquiring should give their number and that should be passed on to the person about whom the call was made. In that way, the parishioner can make their own decisions about whether to be in touch with the telephone enquirer.

10. Parish files which are stored electronically including but not limited to parish lists with unlisted telephone numbers should be password protected.

11. As per the Diocesan Gray Book #4-3B with regards to parish information, the principles recommended to a parish in determining whether or not to provide access to personal information are:

- A person or family should be given access to entries containing their own information
- Others should not be given this information without the specific, written permission of the person or family to whom it relates.
- While on may wish to encourage legitimate historical research and such researchers may be given access to parish records, it is for the Officers of the

parish to decide what constitutes legitimate research and which specific requests to grant.

PARISH RECORD KEEPING RESPONSIBILTIES WITH REGARDS TO EMPLOYEES IN ACCORANCE WITH THE EMPLOYMENT STANDARS ACT – ONTARIO

The following is excerpted from "Your Guide to the Ontario Employment Standards Act" (p.9) with regards to record keeping in the parish.

"All employers in Ontario are required to keep written records about each person they hire. These records must be kept by the employer, or by someone else on behalf of the employer, for a certain period of time. The employer must also ensure that the records are readily available for inspection."

Contents of employee records

Each employee's written record must contain several pieces of information.

The employee's name, Address and Starting Date of Employment. This must be kept for three years after the employee stopped working for the employer.

The employee's date of birth if the Employee is a Student under 18. This must be kept either three years after employee's 18th birthday or three years after the employee stopped working for the employer, whichever happens first.

The Hours Worked by the Employee Each Day and Week. This must be kept for three years after the day or week of work.

If an employee receives a fixed salary for each pay period and the salary doesn't change (except if the employee works overtime) the employer is only require to record:

- The employee's hours in excess of those hours in the employee's regular work week;

AND

- The number of hours in excess of eight per day (or in excess of the hours in the employee's regular work day, if it's more than eight hours).

Employers aren't required to record the hours of work for employees who are exempt from overtime pay and the provisions for maximum hours of work.

All the Vacation Time Taken by the Employee - this must be kept for three years after the vacation time was taken

The Information Contained in an Employee's Wage and Vacation Pay Statements – this must be kept for three years after the information was given to the employee.

All the Documents Relating to an Employee's Pregnancy, Parental or Emergency Leave – these must be kept for three years after the day the leave expired

PARISH PRAYER LISTS:

Public hospitals, nursing homes etc. are covered under the Provincial Privacy Act with regards to Health Information. The Diocese has chosen to develop policies (with help from work from the Diocese of Toronto) in consideration of the Federal Privacy Act. Although it has not been tested in the courts as to whether Religious organizations who have 'members' who choose to be members and by so choosing are making their information available to other members of the 'organization' are actually covered in the Federal legislation, we as a Diocese have chosen to develop these policies in order to be good Christians in ensuring the confidentiality of our parishioners and employees. As it states in the introduction to this Privacy Policy: *The Diocese of Huron is committed to providing ministry to all persons. In order to provide a secure and confidential environment in which we can proclaim the Gospel of Christ with integrity and respect, it is necessary to take measures that will provide a level of confidentiality and privacy to all those who seek our ministry and for those who do ministry.*

So how does this affect our prayer lists?

It has *always* been appropriate for the person who is being prayed for to be asked if she/he would like her/his name (ask about first or first and last) placed in the bulletin and/or on the parish prayer list and to ask about how much information can be shared. This is not different. You are asked to use due diligence to ensure that the person gives permission. You do not need to have them sign a document. If a member of a congregation would like a family member or friend prayed for by the parish community, that member needs to be asked if they have the permission of the family member/friend to put their name forward. This also affects praying aloud the names of those for whom we are concerned—perhaps utilizing first names only can assist with this issue.

It has always been appropriate to ask a person's permission before sharing any of their personal information i.e. health and other person concerns before sharing that information with any others. This continues to apply no matter where you have learned the information—either from that individual, from other congregants, from the hospital, etc.

It continues to be true that when a clergy visits a hospital, they may gain information regarding a parishioner that they didn't have before they went to the hospital. Even the fact that the person is a patient in the hospital is confidential information unless you have their permission to share that information.

When visiting the hospital, you may discover that other parishioners are also patients. You have gained this information from the hospital and because of the Privacy Act that governs hospitals,

you need that patient's permission to share the information or **you may have your privileges suspended at the hospital.**

Diocesan Privacy Officer:

As of January 14, 2004, the Interim Privacy Officer for the Diocese of Huron is The Rev'd Canon Janet Griffith Johnson. She can be reached at (519)434-6893 ext: 224 or in Ontario 1(800)919-1115 or jgriffith@huron.anglican.ca.

The Diocese of Huron recognizes and thanks the Diocese of Toronto for their work on this document and thanks them for permission to use their work in development of our policy.
