



Christ the King Anglican Church

Privacy Policy

Approved by Parish Council
February 2010

Table of Contents

- 1. BACKGROUND..... 3**
- 2. TEN PRINCIPLES..... 3**
- 3. COLLECTION OF INFORMATION..... 4**
- 4. CONSENT 4**
- 5. USE OF INFORMATION 5**
- 6. STORAGE OF INFORMATION 5**
 - 6.1 PAPER RECORDS6
 - 6.2 ELECTRONIC RECORDS.....6
 - 6.3 TEMPORARY STORAGE6
 - 6.4 PERMANENT STORAGE.....6
 - 6.5 TRANSITION TO NEWLY APPOINTED COMMITTEES / OFFICERS.....6
- 7. TIME PERIOD FOR STORAGE OF INFORMATION 7**
- 8. DISPOSAL OF INFORMATION..... 7**
- 9. APPOINTMENT OF A PRIVACY OFFICER 7**
- 10. ACCESS TO PERSONAL INFORMATION..... 7**
- 11. COMPLAINTS..... 7**
- 12. AWARENESS OF PRIVACY POLICY 8**
- 13. PERIODIC REVIEWS OF POLICY 8**
- 14. FURTHER INFORMATION..... 8**
- 15. CONTACT INFORMATION FOR CONCERNS..... 8**
- 16. FORMS 9**
 - 16.1 REQUEST TO ACCESS PERSONAL INFORMATION AND/OR REQUEST TO CORRECT PERSONAL INFORMATION (PIPA)9
 - 16.2 OIPC COMPLAINT FORM (PIPA)10
 - 16.3 OPIC GUIDELINE PROTECTING PERSONAL INFORMATION OUTSIDE THE OFFICE.....13
- 17. REFERENCES 16**
- 18. TERMS OF REFERENCE PRIVACY OFFICER 17**

Privacy Policy

1 Background

Legislation called the *Personal Information Protection Act* (PIPA) came into effect in British Columbia on January 1, 2004.

PIPA governs how private sector and not-for-profit organizations may collect, use, or disclose information about individuals. Among other objectives, the Act seeks to provide a safeguard against “identity theft.” PIPA seeks to strike a balance between the rights of individuals to control the access to and use of their personal information, with the needs of organizations to collect and use such information for legitimate and reasonable purposes. The Act gives individuals the right to see, and request corrections to, personal information held by organizations. If individuals have objections to the ways in which their personal information is being collected and used, they have the right to complain to the Information and Privacy Commissioner (OIPC) of British Columbia.

Organizations are accountable for the personal information they collect, use and disclose. They are accountable for personal information in their custody or control. Organizations have custody of personal information when it is in their offices, facilities, file cabinets and computers, and so on.

Personal information is, generally, under the control of an organization when the organization can decide how to use or disclose the information, how to store it and how long to keep it.

It is important to note that the requirements of PIPA extend to the use of photographs and videos, directories, and websites.

2 Ten Principles

There are ten principles recognized for the protection of privacy and available through the OIPC website. They need no further comment in this document.

- Be accountable
- Identify the purpose
- Obtain consent
- Limit collection
- Limit use, disclosure and retention
- Be accurate
- Use appropriate safeguards
- Be open

- Give individual access
- Provide recourse

Christ the King Anglican Church (the Church), including its employees, leaders and volunteers will adhere to the provisions of the *Personal Information Protection Act* (PIPA) relating to the collection, accuracy, protection, use retention, archival transfer and disclosure of personal information.

3 Collection of Information

The Church will limit its collection of personal information to that which is necessary for maintaining the Parish membership and carrying out the ministries of the Church.

Personal information collected will be provided by the individuals themselves or be reasonably available to the public, such as in the phone book. The personal information collected by the Church includes:

- Name
- Address
- telephone number(s)
- other contact information when it is provided by the individual
- employee information, volunteer information, their applications for employment, screening notes and assessment, and payroll information
- photographs that may be used in a Church directory or for informal records of Church events
- other openly requested information for the purpose of carrying out the ministry of the Church

Only a reasonable amount of personal information will be collected, and will be provided by the individual directly. In situations where the individual is not able to provide contact information, a close personal friend or relative may provide this information, providing it is reasonable to believe that the individual wishes to be included in Church ministries.

Personal information collected for the implementation of payroll, clergy licenses and other formal processes shall be kept confidential and not disclosed to any party other than those who require the information for the purpose for which it was gathered.

4 Consent

Consent is deemed to have been granted if the individual provides the personal information themselves. Completion of our Registration Form and submitting it to the Church office is deemed to be consensual, not only for inclusion in the membership roll but also for inclusion in the Church Directory. It is also deemed consensual for publishing in bulletins and

announcements that are distributed to our membership on Sundays and other ministry gatherings.

PIPA extends to the use of photographs and videos, and church websites. Photographs that will be published on the Church website require that every individual in the photograph provide consent in writing. Other personal information to be published on the website, including personal telephone numbers, also requires consent in writing.

Individual photographs require written consent if they are to be published.

The Church will disclose personal information when is it required in a court proceeding or other legislative process such as an audit.

5 Use of Information

The Church uses personal information it has collected to compile a membership list and to organize the activities of the Church by ministry. Generally, it is collected as contact information to enable ministry groups to enact their ministries.

The Church publishes a Church directory that lists the name, address, telephone number, and email contact information of the members of the Church. The Church directory is available to members of the Church who are in positions of leadership and require this information to facilitate their ministry.

Personal information collected by the Church will never be sold to a third party.

Clergy and pastoral care leaders may use personal information to determine appropriate ministry to provide to the individual. This type of personal information will be kept confidential. In an exceptional circumstance, personal information may be made available to a next of kin or friend of an injured, ill, or deceased individual.

In general, individuals are permitted to access their personal information from the organizations that have requested and collected the information, and they may ask for corrections to that information.

6 Storage of Information

The Church must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

Personal information collected must be destroyed, erased, or made anonymous once the Church no longer needs the information for the purpose for which it was collected.

Generally, personal information that has been collected through the office is kept in locked filing cabinets in the Church Office. Information is also stored in electronic format on the password-protected Church computers.

In a volunteer-powered organization such as the Church, personal information may be disseminated throughout the network of groups and ministries. All team leaders will be required to become familiar with the principles of PIPA and the Church Privacy Policy.

6.1 Paper records

Paper records of membership and contact information are stored in locked filing cabinets. In situations where a member has this information at home, reasonable security and limited access to the location of the information is expected.

6.2 Electronic records

Electronic records of personal information are kept in the Church office on password-protected computers, with firewall and anti-virus software. In situations where a member has this information at home, reasonable password security and limited access to the computer location where the information is stored is expected.

6.3 Temporary Storage

Temporary storage of personal information is not encouraged, although it may be necessary. The reader is referred to an article, found in section 16 of this Privacy Policy, entitled "Protecting Personal Information Outside the Office" published by OIPC. Essentially it is necessary to take reasonable precautions against accident, theft, and other breaches that may cause our personal information to be accessed by an unintended recipient.

6.4 Permanent Storage

Permanent storage of all information, at present, is in the Church office; however it may become necessary or desirable to situate sensitive permanent records elsewhere.

6.5 Transition to newly Appointed Committees / Officers

It is recognized the ministry groups often operate out of their homes. It is the responsibility of every ministry team leader and member to ensure that when they are no longer serving on the ministry team, they pass on the paper and electronic records to the new team members or leaders, and that they destroy all personal information they may have collected during their term.

At the end of the term as leader of a ministry team, all minutes, documents, and records shall be provided to the Church Office for archival and legislative record keeping.

7 Time period for Storage of Information

Records required to meet legislative compliance shall be kept by the Church office in accordance with the requirements of the legislation that applies.

8 Disposal of Information

When a document is no longer needed, paper that contains personal information including name, phone number, address, or other personal information will be shredded before being recycled. This applies to letters, printed emails, notes and any other paper that could identify an individual.

In the situation where a member has paper records at home and has a shredder, they are expected to perform to the same standard. If no shredder is available, all paper records that contain personal information are to be brought into the Church office where they will be shredded and recycled.

When a computer hard drive is replaced, the personal information stored on the drive must be erased or the drive re-formatted before it is sold, recycled, or given to a third party.

9 Appointment of a Privacy Officer

Parish Council shall appoint a privacy officer annually. The appointment shall be disclosed at the annual Vestry meeting to the membership, to ensure widespread awareness, and shall be listed in the Church records of appointment.

Terms of Reference for the Privacy Officer are found in section 18.

10 Access to Personal Information

All individuals have access to the personal information the Church has on file about them, how it is used, and to whom it has been disclosed. The Church recognizes the requirement to help individuals with a request of this nature and will comply with such requests on a priority basis within 30 days. There shall be no fee for this service.

A form entitled "Request to Access Personal Information and/or Request to Correct Personal Information" is found in section 16 of this Privacy Policy. It shall be made available to any member who wishes to request or correct personal information held by the Church.

The Church recognizes the responsibility to do their best to maintain current and accurate information. Corrections will be made as soon as reasonably possible.

11 Complaints

All complaints about unacceptable disclosure of personal information will be treated seriously. All complaints will be investigated by the Privacy Officer. If a resolution cannot be found, the complainant will be referred to the provincial Office of the Information and Privacy Commissioner (OIPC) for formal investigation.

A form entitled “OIPC Complaint Form” is included in section 16 of this Privacy Policy. It shall be made available to any member who wishes to file a complaint with the OIPC. All complaints will be investigated and a resolution sought.

12 Awareness of Privacy Policy

Ensuring widespread awareness of the privacy policy, especially insofar as its protections and rights apply to individuals, and its obligations and procedures apply to the Church, is an essential component of compliance and effectiveness in this area.

The Privacy Officer appointed by Parish Council must be available to all members of the Church, and the Church office must be familiar with the policy and procedures.

It is important to recognize that memories fade and people transition. Accordingly, one of the responsibilities of the Privacy Officer is to organize an annual retraining session for staff and leaders. In addition, the Privacy Officer should ensure periodic reviews of the adequacy and currency of the guidelines and procedures associated with this Privacy Policy.

13 Periodic Reviews of Policy

It is the Privacy Officer’s responsibility to ensure periodic reviews of the adequacy and currency of the guidelines and procedures associated with this Privacy Policy. The annual review is to be summarized and presented in a report to Parish Council, for ratification or further action.

14 Further Information

For further and more detailed information, the reader is referred to review PIPA and to visit the OIPC website, cited in the References section. Other references that are useful are also found in the reference section of this Privacy Policy.

15 Contact Information for Concerns

The address of Christ the King Anglican Church is 2185 Theatre Lane, Victoria BC V8R 6T1. The phone number is Phone 250-519-0130.

16 Forms

16.1 REQUEST TO ACCESS PERSONAL INFORMATION and/or REQUEST TO CORRECT PERSONAL INFORMATION (PIPA)

CHRIST THE KING ANGLICAN CHURCH			
NAME			
ADDRESS			
Street, Apt. #; PO Box #; RR #	City / Town	Province/Country	Postal Code
YOUR TELEPHONE / FAX NUMBER(S)			
Day Phone No. ()	Alternate Phone No. ()	Fax No. ()	
DETAILS OF REQUESTED INFORMATION			
I am requesting access to the following personal information: <i>[Please describe the record(s) you are requesting]</i>			
<input type="checkbox"/> I am requesting information about the way my personal information referred to above has been and is being used by the organization.			
<input type="checkbox"/> I am requesting the names of individuals and organizations to whom the personal information referred to above has been disclosed by the organization.			
I am requesting the organization correct my personal information in the following manner: <i>[Please provide details as to why you think there are errors or omissions concerning your personal information.]**</i>			

**** Please attach a letter if there is not enough room on this form.**

Signature:

Date:

16.2 OIPC Complaint Form (PIPA)

OIPC COMPLAINT FORM

Instructions: Use **this form** to start a privacy complaint or a request a review of an organization's response to your personal information access request to the Information and Privacy Commissioner for British Columbia under the Personal Information Protection Act.

Do not use this form if your privacy issue is with a government or other public body. The Personal Information Protection Act and **materials that may assist you** in completing this form are available at <http://www.oipc.bc.ca/private/> or by calling (250) 387-5629 in Victoria. For toll-free access call Enquiry BC in Vancouver at: (604) 660-2421 or elsewhere in BC at 1-800-663-7867 and ask to be transferred.

Privacy Notice Be aware that a **copy of this form will be provided** to the organization **if your dispute involves a denial by the organization to allow access to your personal information. A copy of this form may be provided to the organization if your complaint is about anything else.**

The information you provide on this form, attach to this form, or provide later to this office will only be used to attempt to resolve your dispute

Send Intake Form to:

Office of the Information and Privacy Fax: (250) 387-1696
 Commissioner for British Columbia Phone: (250) 387-5629 (Victoria)
 PO Box 9038, Stn. Prov. Govt.
 Victoria, B.C. V8W 9A4

We cannot accept complaints or requests for review by electronic mail.

Box below reserved for OIPC date stamp Box below reserved for OIPC staff Name:

Mailing Address: _____

City: _____ Province: _____ Postal Code: _____

Contact Phone No: _____ (include area code) extension # _____

Alternative Phone No: _____

Fax No: _____ Email Address: _____

1. Are you making this complaint or request for review:

on behalf of yourself?

on behalf of another individual?

(Attach supporting documentation if you checked "on behalf of another individual.")

2. Name the organisation your question, complaint, or request for review is about.

3. Summarize your complaint or request for review. *(Please indicate any file or reference numbers and relevant dates)*

4. Tell us about the steps you have taken to try to resolve your complaint:

- Have you attempted to resolve the matter with the organization? Yes No
- Did you write to the organization outlining your concerns? Yes No
- Did you write to object to the organization's initial decision? Yes No
- If yes to any of the questions above, when was the last communication from the organization and what was the result?

5. Who have you dealt with at the organization to try to resolve your complaint or access request?
(List the names, titles, phone numbers, or addresses of people you have had contact with.)

6. Does the matter relate to: (Note: You can choose more than one, if applicable)

- a. **Collection** of Personal Information
- b. **Use** of Personal Information
- c. **Disclosure** (e.g., sharing with others outside the organization) of Personal Information
- d. **Your request** to access your Personal Information
- e. **Your request** to know what has been done with your Personal Information
- f. **Your request** to correct your personal information
- g. **A fee** that has been levied in response to your request to access your personal information

7. Why do you believe the organization's actions are unlawful or in violation of the Personal Information Protection Act ?

If you selected d) or e) or f) in question 6, have you received a written decision from the organization? Yes No

If "yes", what is the date of the letter and when did you receive it? _____

8. Where did the transaction or situation you are referring to occur? (Name prov, territory or country)

9. Do you believe your personal information was sent outside the province? Explain.

10. How do you think this Office can assist you? Describe the result or outcome that you seek.

11. Are you, or were you, an employee of the organization? Yes No

12. Have you contacted or made a Complaint or an appeal to a privacy commissioner in another Canadian jurisdiction regarding this situation? Yes No

If "Yes", name the province or "Canada" for federal commissioner:

Signature: _____ Date: _____

Attach copies of the following documents if you have them:

- Your request to the organization for your personal information or information relating to how your personal information was used or disclosed
- The organization's response to your request
- Your letter of complaint to the organization
- The organization's response to your complaint
- Your letter from the Office of the Information & Privacy Commissioner requiring you to attempt to resolve your dispute with the organization
- Any other correspondence between you and the organization on this matter
- Any documentation that indicates that you are authorized to act for another individual
- The organization's privacy policy and practices (optional)
- Other _____

(Also Print Name)Received by:

Initials: _____

16.3 OPIC Guideline Protecting Personal Information Outside The Office

PROTECTING PERSONAL INFORMATION OUTSIDE THE OFFICE

Whether you're travelling with personal information or working with it at home or another location, personal information can more easily be lost or compromised when it's outside your office. Common sense measures can and should be taken to reduce risks to personal information in such situations.

Private sector organizations covered by the *Personal Information Protection Act* (PIPA) and public bodies covered by the *Freedom of Information and Protection of Privacy Act* (FOIPPA) must take reasonable measures to protect personal information from risks such as unauthorized collection, use or disclosure and are legally liable if they fail to do so. This document offers tips on some steps that can be taken to protect personal information when you take it outside the office and tips on protecting personal information when you're working with it at home.

The following tips apply to "personal information", which is "information about an identifiable individual". The word "organization" is used below to refer to both organizations under PIPA and public bodies under FOIPPA

This document has benefited from a similar publication of the Office of the Information and Privacy Commissioner for Ontario.

Please read the important notice at the end of this document about the nature and status of this document.

WORKING WITH PERSONAL INFORMATION OUTSIDE THE OFFICE

- Never travel with personal information unless you absolutely must have it with you. If you take personal information with you, take the least amount that you need and leave the rest behind. If possible, you should only take copies, leaving original documents in the office.
- While away from your office or your home, laptops and other electronic devices containing personal information (including PDAs such as Palm Pilots and Blackberrys) should be kept with you. If you must leave a laptop or other device somewhere, make sure it is in a location secure from theft, loss and unauthorized access to personal information. (See below for more.)
- Laptops and other electronic devices such as PDAs should be password protected.
- Access to personal information should be password protected, including when stored on a password-protected storage device such as a floppy disk, CD or USB storage drive, rather than the hard drive of your laptop or home computer.
- Electronic records of sensitive personal information when taken away from the office should be encrypted.
- While away from your office or your home, storage devices containing copies of personal information should be kept in a locked briefcase or other container that is kept with you. If you must leave a storage device somewhere, do so in a location secure from theft, loss and unauthorized access to personal information.
- When working outside the office, log off or shut down your laptop or home computer when you're not using it. Set the automatic logoff to run after a short period of idleness.

- When working outside the office, protect your laptop by using locks and alarms as appropriate. As best you can, you should always keep control of your laptop. If this is not possible, you should store your laptop in a secure location such as a locked room or desk drawer.
- Do not share a laptop used for working with private information with other individuals, including family members and friends.
- If the records you need are too voluminous to carry with you, send them to your destination by a trustworthy courier.
- You should avoid viewing personal information in public, including while travelling on airplanes, trains, buses and public transit. Do so only if you absolutely must and take precautions to ensure no one else can view the personal information. For example, your laptop screen should not be viewable by fellow passengers. Set your laptop's screensaver to run after one minute of idleness. Also consider installing a privacy screen filter on your laptop screen, to hinder viewing of the screen from an angle.
- When in transit or working outside the office, avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard and can be intercepted.
- You should avoid discussing personal information in public, including buses, commuter trains, subways, airplanes, restaurants or on the street. If you must do so, ensure others cannot overhear.
- When travelling or working outside your office you should keep personal information under your control, including during meals and other breaks. If this is not possible, store the personal information in a secure location, such as a locked room or desk drawer. Do not leave personal information in plain view or unattended in an insecure place, such as an unlocked office or meeting room.
- Do not leave records containing personal information in plain view in your hotel room. Consider storing the records at a local office of your organization overnight. If your hotel room or hotel office has a safe, store the personal information there.
- Records containing personal information have gone missing over the years when locked vehicles have been broken into or the vehicle has been stolen. Although the trunk of a vehicle is generally considered more secure than the interior of a vehicle, records have been stolen from locked trunks, so extreme caution must be exercised. Records should only be left in a vehicle if there is no other option. They should be locked in the trunk, not left in plain view in the vehicle interior. They also should be left only if the vehicle is parked in a secure location and then only for brief periods. If a staff person must travel regularly with personal information, a car alarm should be installed to enhance the security of records while in transit.
- When working at home, you should store personal information in a locked filing cabinet or desk drawer when not being used. The filing cabinet or desk should only contain work-related records and no one else should have access to it.
- You should avoid storing personal information on the hard drive of your home computer. Any personal information that is stored on hard drives should be encrypted and password protected. You should ensure your home computer has effective Internet security measures such as anti-virus software and firewalls.
- If you telecommute from home, your employer should provide you with a separate phone line and password-controlled voice-mail box.

- You should avoid sending personal information by email or fax from public locations, including Internet cafes. If it is absolutely necessary to do so, see the tips on email and faxing in other OIPC website resources.
- You should fax or photocopy personal information yourself when working outside the office. If you have to ask someone else to do this for you, you should be present.
- Upon returning to the office, return records to their original storage place as soon as possible or destroy the copies securely. Any working notes you created during the trip that contain personal information should also be stored in a secure environment as soon as possible.
- If personal information is stolen or lost, immediately notify your supervisor and the person responsible for privacy compliance in your organization, file a police report, and notify the OIPC. Your organization or public body should consider notifying the individuals whose personal information has been stolen or lost, telling them the kind of information that has been compromised and steps that are being taken to recover it.

OTHER RESOURCES

Other resources are available to help you meet your obligations regarding working with personal information away from your office, including the following:

Office of the Information and Privacy Commissioner, *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office*:

<http://www.ipc.on.ca/images/Resources/wrkout-e.pdf> This document is for general information only. It is not intended to be, and cannot be relied upon as, legal advice or other advice. Its contents do not fetter, bind, or constitute a decision or finding by, the Office of the Information and Privacy Commissioner (OIPC) with respect to any matter, including any complaint, investigation or other matter, respecting which the OIPC will keep an open mind. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization and public body.

17 References

1. *Freedom of Information and Protection of Privacy Act* (FIPPA) and *Personal Information Protection Act* (PIPA) [SBC 2003 Chapter 63] Assented to October 23 2003
http://www.oipc.bc.org/legislation/PIPA/Personal_Information_Protection_Act.htm
2. *Streamlining British Columbia's Private Sector Privacy Laws Report Fourth Session, Thirty-eighth Parliament April 2009* <http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/reports/PDF/Rpt-PIPA-38-4-2008-APR-17.pdf>
3. A Guide To Access to Information and Privacy Protection under BC's Freedom of Information and Protection of Privacy Act June 2004
<http://www.oipc.bc.org/pdfs/public/GuideToFOIPPAJune2004.pdf>
4. Guidelines for Developing a Privacy Policy Under the Personal Information Protection Act (PIPA) May 20, 2004 Office of the Information and Privacy Commissioner for British Columbia <http://www.oipc.bc.org/pdfs/private/PIPAprivacypolicyguidelines051804.pdf>
5. A Guide for Businesses and Organizations to British Columbia's Personal Information Protection Act February, 2005 (3rd Publication) Published by the Office of the Information & Privacy Commissioner (OIPC) for British Columbia (attached)
[http://www.oipc.bc.org/pdfs/private/a- GUIDE TO PIPA\(3rd_ed\).pdf](http://www.oipc.bc.org/pdfs/private/a- GUIDE TO PIPA(3rd_ed).pdf)
6. Personal information Protection Private Sector Policy Implementation Tools Ministry of Management Services no date
<http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/PIPAtoolsPnt.pdf>
7. Faxing and emailing Personal Information February 2005 Office of the Information & Privacy Commissioner (OIPC) for British Columbia (attached)
[http://www.oipc.bc.org/pdfs/public/fax-emailguidelines\(Feb2005\).pdf](http://www.oipc.bc.org/pdfs/public/fax-emailguidelines(Feb2005).pdf)
8. Protecting Personal Information Outside the Office February 2005 Office of the Information & Privacy Commissioner (OIPC) for British Columbia (attached)
[http://www.oipc.bc.org/pdfs/public/PersonalInfoOutsideOffice_\(Feb2005\).pdf](http://www.oipc.bc.org/pdfs/public/PersonalInfoOutsideOffice_(Feb2005).pdf)
9. Request to Access personal Information and/or Request to Correct Personal Information OIPC <http://www.oipc.bc.org/HelpfulForms.htm>
10. OIPC Complaint Form OIPC
[http://www.oipc.bc.org/pdfs/private/OIPC%20Complaint%20Form%20\(PIPA\)%20-%20\(FINAL\).pdf](http://www.oipc.bc.org/pdfs/private/OIPC%20Complaint%20Form%20(PIPA)%20-%20(FINAL).pdf)
11. How to File a Complaint with an Organization OIPC
http://www.oipc.bc.org/pdfs/private/privacy_complaint_resolution_form.pdf

18 Terms of Reference Privacy Officer

Privacy Officer

Terms of Reference

The Privacy Officer shall be appointed by Parish Council and their appointment confirmed at Vestry annually.

The term of appointment is one year, reviewed and renewed annually if appropriate. There is no limitation to the number of consecutive terms the Privacy Officer may hold the position.

The Privacy Officer must:

- Ensure widespread awareness of privacy policy and complaint process to all members of the Church and particularly to staff and ministry leaders.
- Act as a confidential, if requested, advisor to those seeking information or with concerns about privacy breaches
- Make readily available request for Information forms and Complaint forms to any enquiring individual
- Ensure an appropriate investigation is launched when a request of complaint is launched
- Keep accurate records of privacy concerns and complaints, providing them to the office as required
- Annually review Church policy and procedures to ensure compliance is met and the Church members needs are met
- Make recommendations to Parish Council for revisions to Privacy policy
- Surrender all records to the Church office for storage upon completion of appointment
- Act as a liaison between an individual, the Church and the OIPC when required.

This position is responsible to Parish Council and the congregation.