

Final Privacy Policy Version 4

**Main-Gerrard Community Development Co-operative, Inc.
[Main-Gerrard Housing Co-op]**

Privacy of Personal Information Policy

Approved by the Board of Directors: July 11 2005

Main-Gerrard Housing Co-op collects a great deal of personal and sensitive information on members during the application process and throughout the duration of the occupancy. We also have personal information on staff [not covered by PIPEDA, but other statutes/agreements do have restrictions].

The Co-op must comply with the Federal *Privacy Information Protection and Electronic Documents Act (PIPEDA)*, which applies to the standards for personal information with respect to commercial activity.

We believe this policy meets or exceeds the requirements of the *Privacy Information Protection and Electronic Documents Act*.

The collection and storage of personal information should be treated in a manner that is respectful of the individual and conforms to the Privacy Principles attached as Appendix A.

Privacy Officer

The Board of Directors shall act as the Privacy Officer of the Co-operative. The Board of Directors will be responsible for the organization's compliance with all privacy legislation.

The Privacy Officer's duties are to:

1. review the Co-op's policies and practices with regard to personal information
2. recommend implementation of the necessary changes to guarantee that the collection and retrieval of personal information follow the Co-op's policy and PIPEDA. The Privacy Officer will use the 10 Principles and the published Findings of the Privacy Commissioner for guidance in addressing policy changes or complaints.
3. inform the members and public on how the Co-op treats personal information
4. handle complaints following the 10 principles contained in PIPEDA.
5. *where the the Board of Directors acting as the Privacy Officer is not able to resolve a complaint, then the Directors may decide to seek outside assistance [legal advice, contacting the Privacy Commissioner office, mediation, etc.]*

Definition of Personal Information

For the application of this policy, personal information means:

1. The personal address, telephone number or email address of the individual
2. Any identifying number assigned to an individual which can lead to their identification (e.g. Social Insurance Number)
3. Information about an individual's income and assets
4. Bank account and credit card information
5. Information about housing charge payment history

6. Information relating to the race, national or ethnic origin, citizenship status, colour, religion, age, sex, sexual orientation, marital or family status of the individual
7. Information relating to the education, medical, psychiatric, psychological, criminal or employment history of the individual
8. Credit and rental history reports
9. Financial information for the purposes of establishing Rent-Geared-to-Income Assistance
10. An individual's blood type or fingerprints
11. Information about an individual's personal or political opinions
12. Correspondence sent to the co-op that is of a private or confidential nature, and any replies from the co-op that would reveal contents of the original correspondence
13. The individual's name if it appears with other confidential information (e.g. housing charge arrears reports)
14. Employee information including résumés, salary and benefits [aggregate information required for budget or audit purposes is not disallowed], disciplinary action, bank account information, member complaints about the individual, and problems between staff.
15. Any other personal information not covered by the above.

Personal information does NOT include the name, position and business phone number of employees.

Personal information does NOT include statistical data, which is summarized in such a way as to not identify any individuals.

Business contact information and certain publicly-available information such as name, address and telephone number (as published in telephone directories) are not considered personal information.

Collection of Information

Personal information will be collected only for the following purposes:

1. to approve membership
2. to determine appropriate unit type and size
3. to determine income and assets for housing charge calculation
4. to demonstrate compliance with requirements contained in the Operating Agreement.
5. to protect the health and safety of the member
6. to conduct reference and employment checks
7. to retain relevant information on employees for government reporting purposes

The Co-op must not seek out personal information about members or applicants unless it is directly relevant to the purposes stated in this policy.

All documents used for collection of personal information shall state

- a. the purpose or purposes of the collection;
 - b. the reasons for collection, including the fact that the information may be shared as necessary for the purpose of making decisions or verifying eligibility for assistance under the Community Sponsored Housing Program [through Canada Mortgage and Housing Corporation], the *Ontario Disability Support Program Act, 1997*, the *Ontario Works Act, 1997* or the *Day Nurseries Act*.
 - c. the name, title, business address and business telephone number of the Privacy Officer who can answer questions and respond to complaints about the collection, use or disclosure of the information;
- and will include
- d. a consent form to be signed by the applicant or tenant authorizing the collection, use, verification and disclosure of the information being collected

Protection of Information

All board members will be required to sign a confidentiality agreement.

Applicant, member and employee files (including information on databases) must be safeguarded against unauthorized access.

Applicant/member information and employee information must be stored in a locked filing cabinet. Secure storage facilities must be provided for archived applicant/member/employee and accounting information.

Staff and members of the Board, where appropriate, should have access to records containing personal information only if required in order to fulfil their duties.

When communicating member issues to the Board, staff should use non-identifying information wherever possible. For example, arrears reports should use a consistent coding formula in place of the actual names of members.

Databases containing files with personal information, and other confidential electronic files must be password protected against unauthorized access.

Screen-savers or other protective action will be used to protect confidentiality of personal information on computer monitors.

All staff have a responsibility to ensure that unauthorized individuals do not have unsupervised access to areas where files are kept and used.

Personal information will be disposed of at the end of the required storage period for member records of 5 years after the member has moved out, and for financial records of 7 years after the end of the fiscal year. The accounting program at present does not permit deleting account information so only the Co-ordinator, bookkeeper and auditor will be provided with access to the books.

Paper-based personal information must be shredded prior to disposal. Electronic media must be *disposed of in a way that ensures protection of personal information*.

Release of Information

No personal information will be released to third parties without the written consent of the individual (for example: credit references, member or personal references). When responding to enquiries for references, staff should limit information provided to the questioner and confirm only the information already provided by the individual making the inquiry.

It is not necessary to have a signed consent to release information to collect a debt, for example to a collection agency, or for an eviction proceeding or Small Claims action.

Staff will take reasonable care to confirm the identity of the people to whom information is released.

Personal information will be released to the following:

1. Funders and Auditor: The Co-op, in order to be in compliance with funding program requirements, must release information to funders and auditors. People doing these jobs have their own professional code of ethics and are required to maintain confidentiality. Staff should confirm that the person concerned is seeking access legitimately.

2. Researchers: Occasionally, the Co-op may be asked to assist a researcher who may be from an academic institution or who may be independent. Authorization for such people to have access to files will depend on their credentials and the nature of their research. The Board of Directors must approve all such requests for personal information.

4. Credit Bureaus: Information on orders or judgements for money owing will be provided to any credit bureau of which the Co-op is a member.

5. Law Enforcement: While the Co-op has a responsibility to protect the rights of applicants and members to privacy, this responsibility must be balanced with an obligation to the broader community. Law enforcement agencies requesting personal information about applicants, members or employees, will be required to provide a written request or “warrant” before information will be released.

Personal information may be released to the police:

- i. In the context of reporting criminal activity, staff with personal knowledge should report theft, damage or fraud.
- ii. With respect to crimes against persons, witnesses are obligated to report and provide appropriate information to the police so that charges can be laid. Domestic violence is a criminal offence and should be reported to the police.

- iii. To report suspected criminal activity. If there is good reason to believe that there is a drug problem or *other illegal activity being engaged in by members*, this should be reported to the police.
 - iv. Victims of crimes are responsible for reporting the crime directly to the police. However, if the victim is a child or a person with a disability that renders them incapable of making the decision to report, the legal responsibility lies with the co-op to report the crime to the Police or Children's Aid Society, if it has relevant information.
 - v. In the case of suspected child abuse, information will be provided to the Children's Aid Society. (This duty to report is required under the *Child and Family Services Act*, Section 72.)
6. Health and Safety Officials: Personal information will be provided to outside agencies, individuals and institutions when it can be clearly identified as contributing to the applicant or member's benefit, for example, information about an individual's medical condition to the fire department.
 7. Next of Kin or Emergency Contacts: It may be appropriate to use personal information to contact a community service agency or a designated relative in exceptional circumstances, such as, when using an emergency contact provided by a member and held on file, or contacting medical support services when a member is unable to function and maintain his/her membership.

Retention of Personal Information

The co-op is required to keep certain files for specified periods of time.

Financial records that back-up audited financial statements are to be kept for seven years.

Current member's files are to be kept up-to-date for the previous ten years. Original occupancy agreements are to be kept on file.

The files of past members are to be kept for six months, unless required for debt collection

Applications that the board has rejected are to be kept for six months, or until any appeals have been resolved.

Applications that the board has approved and are subsequently withdrawn by the applicant are to be kept for six months.

Some types of files are to be kept permanently. These include:

Certain types of property information such as property descriptions, drawings and information related to major renovations of the property.

Corporate records such as Articles of Incorporation, minutes of the board and members' meetings and lists of directors.

Other information can be purged according to policies and procedures established by the co-op from time to time.

Access to and Correction of Personal Information

The Privacy Officer will respond to all requests for access to or correction of personal information.

An individual who provides satisfactory identification will be informed of the existence, use and disclosure of his or her personal information and will be given access to that information. The privacy of others' personal information must be protected when giving an individual access to his or her own personal information.

If the Privacy Officer believes that releasing personal information to an individual would prejudice the mental or physical health or security of any person, he or she will not release the information.

An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. If the Privacy Officer is not in agreement with the individual's request for correction, a counter-statement will be filed with the original information.

Privacy Officer & Procedure for Handling Complaints

The Privacy Officer will respond to all complaints about collection, use, disclosure, storage and disposal of personal information within thirty days of the request being made, and advise the complainant as to the action that has been taken.

Each complaint will be assessed to determine whether:

Correction of personal information is necessary.
Information was collected, used, released or disposed of inappropriately.
The co-op's policies and procedures need to be strengthened.
Disciplinary or other action needs to be taken with respect to a breach of a confidentiality agreement.

Where necessary, the Privacy Officer will make the necessary recommendations to the Board of Directors in connection with resolution of the complaint.

Breach of Confidentiality

It is a breach of confidentiality to:

Discuss any confidential information outside the meeting where the information was presented. This would include discussions through the internet.
Provide confidential information or records to unauthorized individuals.
Leave confidential information in written form or displayed on a computer terminal in a location where it may be viewed by unauthorized individuals.

A breach of his or her confidentiality obligation may be grounds for a board member to be removed as a director of the corporation. A board member who breaches confidentiality may not be covered by the co-op's insurance if he or she is sued for libel.

Video Surveillance

Should the Co-operative begin to use video surveillance in any of the common areas of the Co-operative the only purpose for this will be to address a serious concern for safety of members or to inhibit criminal behaviour.

The Privacy Commissioner of Canada has developed criteria for video surveillance. The following five points outline the Privacy Commissioner's test for using video surveillance. The Co-operative shall follow this guideline.

- *Is the measure demonstrably necessary to meet a specific need?
The Co-operative will consider whether the implementation of video surveillance is necessary to meet the specific need it is trying to address.*
- *Is video surveillance likely to be effective in meeting that need?
The Co-operative should consider how effective video surveillance will actually be in addressing its need.*
- *Is the loss of privacy proportional to the benefit gained?
The Co-operative should consider whether the loss of privacy to its members is justifiable given the need it is trying to address by the implementation of video surveillance.*
- *Is there a less privacy-invasive way of achieving the same end?*
- *Lastly, the organization should consider the cost and effectiveness of other less privacy-invasive alternative measures to video surveillance.*

If the members decide to implement video surveillance, the only persons who are able to access the video recordings shall be authorized by the Board of Directors. This person shall ordinarily be the Co-operative Manager. Exceptions will be reported to the full membership. The video recording must be kept in a locked room accessible only to those authorized. Once the video recordings are no longer necessary to meet any security need, they will be erased or deleted or recorded over. The Manager of the Co-operative will be the only person responsible for monitoring, reviewing, accessing and erasing the security recordings.

Audio Recording of General Membership Meetings

All general meetings of members of MAIN-GERRARD COMMUNITY DEVELOPMENT CO-OPERATIVE, INC will be audio recorded. The sole purpose of the audio recordings will be to verify the accuracy of the minutes of the Corporation should there be a challenge to the written minutes. Once the minutes of the recorded meeting have been approved by the members, the audio recording will be erased. No copies of the audio recording will be made.

CONFIDENTIALITY AGREEMENT

The Board of Directors have a more detailed confidentiality agreement and code of conduct that each director or alternate will sign each year. The following confidentiality agreement must be signed by any Committee member who is in regular possession of personal information, such as the Membership Committee.

I understand that in the course of conducting my responsibilities as a director or volunteer of Main-Gerrard Community Development Co-operative, Inc., I may have access to personal information about applicants, members and employees of the corporation. I understand that there are legal restrictions on how this information may be collected, used, stored and disposed of and that privacy of personal information must be respected.

I hereby agree to abide by the co-op's policy regarding confidentiality attached to this agreement and by the restrictions placed on this information by the *Personal Information Protection and Electronic Documents Act* and any other statute which is now or may later be in force.

Dated this _____ day of _____, 20____.

Signature

Appendix A. – 10 Privacy Principles (for more detailed understanding of these Principles, see the Act and the Commissioner’s Findings on the Privacy Commissioner’s web site, www.privcomm.gc.ca).

Principles of Personal Information Protection

The *Personal Information and Protection of Electronic Documents Act (PIPEDA)* is based on ten principles of personal information protection. These principles explain the intent of the Act. This is a brief outline:

1. Accountability

Each organization must appoint an individual, or individuals, responsible for ensuring compliance with PIPA.

An organization is responsible for the personal information under its control. It must implement policies and practices that apply these principles.

2. Identifying purposes

Organizations must identify how they will use information when they collect it.

Organizations must tell individuals why they are collecting personal information.

If an organization want to use information in a different way at a later date, the individual must give their consent

3. Consent

Individuals must know about, and consent to, the collection of personal information about them.

The supply of a product or service may not be made conditional on consent to the collection of non-essential information.

4. Limiting collection

Organizations may only collect the information that is necessary for the identified purposes.

5. Limiting use, disclosure and retention

Organizations may use and disclose personal information only for identified purposes.

Organizations may keep personal information only as long as they need it for identified purposes. They must then destroy it.

If an organization uses personal information to make a decision about an individual, they must keep the information long enough for the individual to have access to the information after the decision has been made.

6. Accuracy

The use of the information determines how accurate and up-to-date the information must be.

Organizations may not update information routinely unless necessary.

7. Safeguards

Organizations must keep personal information secure and restrict access to it.

8. Openness

Organizations must provide information about their policies on the management of personal information. They must indicate who in the organization is responsible to ensure compliance with PIPA (for example, personal information protection policy posted on website).

9. Individual access

When asked, organizations must tell individuals what personal information is held about them and they must allow the individual to check the accuracy of the information.

The organization must correct inaccurate information.

10. Challenging compliance

Organizations must have a procedure in place to receive and handle complaints about how they collect and use personal information.

Appendix B

Access to Files

You have the right under the by-laws to “...see (your) own personal files and financial accounts during co-op office hours.” The Board has enacted a draft policy to outline specifically how this can happen. As with all policies, your feedback and input are invaluable to the Board of Directors and if you would like to see a change to what is below, please drop a note into the office and it will be presented to the Board.

Policy enacted by the Board of Directors re: Member Access to Member Files and Accounts

- 1) *All requests must be in writing and delivered to the Co-op’s administrative office;*
- 2) *Members requesting access to their files must specify two times over the next two weeks, during open office hours, that they would like to come in and see their files;*
- 3) *If the times specified are not possible for office staff, the Manager/Co-ordinator must respond in writing with two alternative times over the same time period;*
- 4) *Once the appointment has been set, if the member doesn’t keep the appointment, the Board must approve any subsequent time;*
- 5) *No documents are to be removed from the member’s files by the member. Members can challenge the need to have an item in the file, and if the Manager agrees that there is no reason to keep the item, the member can either take it with them or the Manager can shred the document*
- 6) *If the member and Manager cannot agree that something in the member’s file doesn’t belong in the file, the member is advised that it is her or his right to appeal the matter to the Co-operative’s Privacy Officer. Members also have the right under PIPEDA to file a complaint with the Privacy Commission of Canada regarding the contents of their file;*
- 7) *Members are not allowed access to the Co-operative’s bookkeeping system.*
- 8) *At all times the privacy rights of other members shall be preserved by staff while a member is in the office looking at their file.. If they request a copy of their accounts as contained within Newviews, which is the bookkeeping program used by the Co-operative, the Manager will provide an up to date print out*

Appendix C

Procedures needed to carry out this policy

1. Determine how personal information and confidential co-op information will be collected, used, filed, shared and protected.
2. Determine who has the authority to access and release different types of personal information (and confidential co-op information).
3. Develop procedures for routinely destroying personal information that the co-op no longer needs.
4. Develop a personal information complaints procedure.
5. Review and revise, as necessary, forms that ask for personal information, e.g. application form.
6. Develop forms for the personal information protection statement (to be signed by applicants) and memo to current members about personal information.
7. Train management staff and members about their responsibilities for protecting personal information.
8. Establish procedures for keeping the confidential portion of minutes secure.