MULTI-SERVICE CENTRE

POLICY MANUAL

Category	Administrative		
Section	Rules/Conduct	**Sub-Section:**	Rules
Number	2-1		

Approved by:  **Approval Date:** March 4, 2019.

Name/Title: Fran Bell, MSC Board Chair
Responsibility of: Kathryn Leatherland
Name/Title: Executive Director
Issued By: Organizational Development
Replaces Policy Dated: October 30, 2014.
Review Due Date: As needed.

PRIVACY AND CONFIDENTIALITY POLICY

Purpose:
In order to provide quality services and care to our clients, the Multi-Service Centre (MSC) is required to collect and use personal information. The MSC is committed to protecting the privacy, confidentiality and security of all information gathered from clients, staff and volunteers. The purpose of this policy is to state the MSC's commitment to ensure compliance with relevant provincial and federal legislation, and therefore preventing the inappropriate collection, use and disclosure of personal information.

Personal information is given to the MSC in trust. It is mandatory that the information remains confidential. It is important that information not circulate outside of the organization in an unauthorized manner, and it also should not pass between staff for reasons other than appropriate consultations.

Scope:
This policy applies to all Board members, staff and volunteers of the MSC. Additionally, the MSC requires that any individual or third-party who collects, uses or discloses personal information on behalf of the organization, complies with the provisions of this policy.

Definitions:
Privacy – the fundamental right of an individual to control information about ourselves (including the collection, use and disclosure of and access to that information).

Confidentiality – an obligation to protect personal information, to maintain its secrecy and not misuse or wrongfully disclose it.

Personal information – Personal information is any information about an identifiable individual, other than an individual's business title, address or telephone number. Examples of personal information are: name, home address, age, health and financial information. It does not include information that cannot be tracked back to a specific individual. In addition, information that is publicly available, such as a telephone book listing, is not considered to be personal information.

- Donors: The history of an individual's donations to the MSC is considered personal information.
- Employee personal information does not include the name, job title, work telephone number or work address, or anything that might appear on a business card.

Personal health information – Personal health information is defined to mean, with respect to an individual, whether living or deceased:

- Information concerning the physical or mental health of the individual;
- Information concerning any health service provided to the individual;
- Information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of an individual;
- Information that is collected in the course or providing health services to the individual; or
- Information that is collected incidentally to the provision of health services to the individual.

Policy Statement:
The MSC will comply with all applicable provisions of privacy legislation, including the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Protection Act (PHIPA), the Personal Information Protection and Electronic Documents Act (PIPEDA) and Canada's Anti-Spam Legislation (CASL).

To achieve its mission, the MSC collects certain personal information about its donors, clients, event participants, staff and volunteers, meeting legal obligations and as otherwise permitted or required by law. Such information enables the MSC to deliver programs and services, pursue government relations and advocacy initiatives, fundraise, process donations, conduct marketing efforts, undertake statistical reporting, etc.

MSC collects the minimum amount of information needed to establish and maintain a service, volunteer, participant, donor or program relationship with an individual. Subject to the application of the consent principle outlined in principle 3 below, personal information collected by the MSC may include, but is not limited to:

- Contact and identification information, such as name, address, telephone number and email address;
- A brief summary of the service(s) requested and or received (programs and services database);
- Case notes or personal health information;
- Participation in MSC campaigns and fundraising events;
- Donation information such as date of gift, amount of gift, the campaign to which one contributed;
- Financial information such as payment methods and preferences, billing and banking information (credit card number and expiry date or chequing account transit numbers which are required to process a donation);
- Other personal information used for purposes that a reasonable person would consider appropriate in the circumstances.

The MSC will abide by the following principles in the collection, use and disclosure of personal information:

1. Accountability
   The MSC is responsible for personal information under its control and must maintain its confidentiality at all times. All MSC Board members, staff and volunteers share this responsibility. Our responsibilities in protecting information also entail the assurance that third parties maintain the same levels of privacy as MSC.

   Board members, staff, volunteers, students and associates with access to client and employee information are expected to comply with the Privacy and Confidentiality policy. As part of their orientation to the MSC they are asked to sign a Confidentiality Agreement indicating they understand and agree to abide by this policy. A copy of the signed statement will be kept in the personnel/HR records. The obligation of confidentiality remains in effect even after termination of employment.

It is the responsibility of the Director of each program to ensure that any person having access to client and employee information is made aware of the policies and procedures concerning confidentiality and that each individual sign the Confidentiality Agreement.

- *The Privacy Officer*
  The Executive Director or designate will act as the MSC privacy official. This Privacy Officer receives senior management support and has the authority to intervene on privacy issues relating to any of MSC's operations. The name or title of this individual will be made available both internally and externally to ensure their accessibility.

  The Privacy Officer is responsible for facilitating the organization's compliance with all privacy-related legislation. He or she responds to client's requests for access to or correction of a record of personal health information and responds to inquiries from staff as well as the public about the Centre's privacy policies and procedures. Finally, the Privacy Officer receives complaints from staff, clients or the public about privacy and confidentiality-related matters.

- *Privacy Training*
  The Privacy Officer is responsible for training and communicating to staff information about the organization's privacy policies and practices, such as their duties under PHIPA and the role of the Privacy Officer.

- *Practices and Procedures*
  The MSC will implement practices and procedures to carry out the policy, including the protection of personal information, receiving and responding to complaints from individuals regarding their personal information, training of Board, staff and volunteers about this Privacy & Confidentiality Policy and procedures and developing information to explain our privacy policy and procedures.

2. <u>Identifying Purposes</u>
   Information will be gathered from the client, participant, employee, volunteer or third party for specific purposes. The MSC will identify the purposes for which personal information is collected. The identified purposes will be specified at or before the time of collection to the individual from whom the personal information is collected. The MSC shall only collect information as needed to fulfill the identified purpose. When personal information that has been collected is to be used for a purpose not previously identified, the MSC is obligated to communicate the new purpose to each individual and obtain their consent to use the information before use.

   Examples of purposes for the collection of information:

   - To provide direct care
   - To contact clients/volunteers regarding upcoming events
   - To submit information required by funding agencies (e.g. Ministry of Health and/or Ministry of Training, Colleges and Universities)
   - To plan programs and services
   - To employ individuals
   - Quality improvement (e.g. Evaluation and chart audits)
   - Any other reason needed to provide services

3. <u>Consent</u>
   The valid and informed consent of the individual are required for the collection, use, or

disclosure of personal information, except where consent is not required by legislation. It is anticipated that instances in which knowledge and consent of the individual would not be required would be extremely rare and would include legal, medical or security reasons which would have to be fully documented. Consent may be express or implied, depending on the circumstances and sensitivity of the information.

Valid and Informed (Express) Consent – Consent is considered valid only if it is reasonable to expect that individuals to whom the MSC's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure, to which they are consenting. Typically, MSC staff will seek consent for the use or disclosure of the information at the time of collection. The client will always be given the opportunity to rescind consent. Consent is valid if it meets the following criteria:

- Consent is voluntary;
- Client has the physical and mental capacity to consent; and
- Client has been properly and meaningfully informed.

Express consent is required from an individual before the MSC will disclose personal health information about an individual to that individual or an external organization.

Competence to Consent – An incapable person cannot provide valid consent. If a practitioner deems a client unable to consent, a substitute decision-maker must then act on his or her behalf. All the rights of the person apply to his/her substitute decision-maker.

Implied Consent – Implied consent occurs through the actions or conduct of the client rather than direct communication through words. The provision of personal information to the MSC for the purpose of receiving service or care constitutes implied consent to collect, use and disclose their personal information in accordance with this policy, unless an individual expressly instructs otherwise.

Implied consent is generally time-limited, to typically 2 years beyond the event that starts a relationship. Implied consent can also be inferred where there is an existing business or non-business relationship between an individual and the MSC. Examples include but are not limited to a donor, a volunteer, a Board member, an event participant, someone who has contacted the MSC for services, etc.

Implied consent is considered to be sufficient for fundraising purposes to allow the trade of limited personal information (name and home address only) about a donor to another charitable organization if the individual has been informed that his/her personal information might be used in this manner and he/she has been given an opportunity in a clear and meaningful way to opt-out.

No consent – There are certain activities for which consent is not required to use or disclose personal information. These activities are permitted or required by law. For example, we do not need consent from individuals to (this is not an exhaustive list) respond to legal proceedings or comply with mandatory reporting obligations, investigations / fraud detection and prevention, witness statements in insurance claims, financial abuse, personal information produced in the course of employment, business or profession, or other as identified by law from time to time. The MSC may use or disclose your personal information without consent where the MSC believes, upon reasonable grounds, that it is necessary to protect the rights, privacy or safety of an identifiable group or person (including you) or the public.

Withholding or Withdrawal of Consent – If consent is sought, an individual may choose not to give consent ("withholding consent"). If consent is given, an individual may withdraw consent at

any time, but the withdrawal cannot be retrospective. The withdrawal may also be subject to legal or contractual restrictions and reasonable notice.

4. Limiting Collection
The MSC will:

- Limit the amount and type of information gathered to what is necessary for the identified purpose.
- Ensure that there is a justifiable purpose for obtaining and recording personal information.
- Not collect personal information by misleading or deceiving individuals about the purpose for which the information is collected.

Information will be collected by fair and lawful means.

5. Confidentiality of Information
The MSC will use or disclose personal information only for the purpose for which it was collected, unless the individual consents otherwise or the use or disclosure is required by law.

Business Affairs
A Board member, employee or volunteer shall not disclose the business affairs of the Centre and shall not use for his/her purposes or the purposes of any other organization or individual any information that s/he may acquire about the operations of the MSC, as per the conflict of interest policy.

Access to Client and Employee Information – Authorized staff
Access to personal information will be limited to authorized users only. Personal information may be used only within the limits of each staff and volunteer role, and staff and/or volunteers may not read, look at, receive or otherwise use personal information unless they have a legitimate need to know as part of their role. Personally identifiable information should be restricted to:

- staff providing service to the client, and their supervisor;
- staff member(s) who are providing assistance to the staff providing service to the client;
- staff assigned to tabulate and collate data;
- appropriate administrative personnel; and
- volunteers who need access to parts of client records to complete their work

Case discussions, consultation, services are confidential. When staff, client or volunteer safety is at risk (reference the Health and Safety Policies and Procedures) this will take precedence. However, in any instance, the minimum amount of information judged necessary to thwart the potential harm is disclosed.

For problem solving purposes or for finding an appropriate resource for a client, staff do not need to identify clients in any way. If staff members have mutual clients, clients can be identified in discussions. Staff consultations are essential for updating providers on new and pertinent information about a client, seeking consultation and supervision in serving a client or developing plans of service or care for a client. However, where necessary and in order to provide clients with comprehensive health care, their personal client information may be shared among those staff members who are directly involved with their care. Sharing of information is done only when necessary and appropriate to provide clients with quality service.

Day to Day Maintenance in the Limitation of Disclosure

- All records are returned to the designated area at the end of the day.
- Appointment and records books are kept closed when not in use and are stored securely when the employee is not at work.

- Cases and clients are not discussed in open areas, such as waiting areas, the kitchen, lunchroom or hallways.
- All telephone conversations are kept as private as possible.
- Client data is never left on computer screens were it could be viewed by a passer-by, nor is it left on any surface in a common or public area, such as the reception desk.

Retention Time
Staff members will:

- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Providers may keep informal notes about their clients (telephone messages, etc.) that are only needed temporarily. While these notes may not necessarily become part of a client's file they should be treated with the same level of confidentiality and with the same confidentiality practices. When discarding informal notes care should be taken to ensure that they are destroyed in an appropriate manner.
- Refer to File Retention, Destruction and Security Policy for additional information regarding retention time.

6. Accuracy
   It is the responsibility of MSC staff to take reasonable steps to ensure that personal information in our custody is accurate, complete and up-to-date as required for the purposes for which it is used. MSC staff will:

   - Create and maintain client records which are clear, concise, comprehensive, professional, and which serve to further the care of the client; and
   - Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

   Individuals always have the opportunity to contact the MSC and update their personal information.

7. Safeguards
   The confidential records as well as other documented information belonging to clients, staff and volunteers are the property of the MSC, whose responsibility it is to take all reasonable precautions to secure the information against loss, fire, theft, defacement, tampering, access or copying by unauthorized persons.

   Security safeguards are intended to protect personal information. Appropriate security safeguards will be used to provide necessary protection, regardless of the format in which it is held, such as physical measures (e.g. restricting access to offices), technological tools (e.g. passwords) and organizational controls (e.g. confidentiality agreements, electronic health records access audit). Employees are to access computers, files and other recorded information of the MSC and its programs, employees, volunteers and clients only as authorized and required for the effective delivery of programs and/or service.

   Telephone, Fax or E-mail Client Information Disclosures
   Information is only disclosed following proper consent practices. Information is never given to anyone if there is any question as to the person's identity (see Electronic Disclosure of PHI Procedure).

   Contracts and Service Agreements
   The MSC requires that any individual or third-party who collects, uses or discloses personal information on behalf of the organization complies with this policy. Written contracts will be issued for all services rendered by third parties (such as paper/document disposal, consultants, cleaners and contractors). A confidentiality clause will be included in the body of the contract.

This clause will clearly outline the obligations of both parties regarding confidential records or document in order to achieve compliance with PHIPA.

Security Measures for the Proper Storage of Information
Secure access shall be assured in all areas where client and employee information records are kept including case files, records stored in computer banks, central file areas and any sub-systems created for convenience.

Locked cabinets, locked shelves or a locked room in which records information is housed will assure security. Client personal information will not be transmitted via email, including names if the email is about client care issues.

Client files will not be removed from the Centre unless the Executive Director provides special authorization. The removal of confidential information in any form from the Centre premises is discouraged and must comply with established practices. Anyone removing confidential information is accountable for protecting such information until it is safely returned to the Centre.

Confidential client information stored in computers and external memory drives (ex: USB sticks) can be accidentally destroyed or stolen. It is the responsibility of all users to protect the information stored on their personal computers. Electronic devices (mobile phones, , laptops, etc.) must be password protected in the event they are lost or stolen. Staff who occasionally work from home must ensure they are working over a secure network and that no one else in the home has access to client information. The more confidential and sensitive the information, the more comprehensive the measures to protect it must be taken.

The photocopying of client records is the responsibility of authorized staff. All copies of information sent outside the Centre must be endorsed with the date the material was sent and contain the label “copy”.

Care will be taken in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information.

8. Openness
The following information will be readily available to staff, Board of Directors, volunteers and clients:
    - information about our policies and procedures relating to the management of personal information;
    - name and contact information for the Privacy Officer (in order to access information, inquire about our privacy policies or make a complaint);
    - a description of the type of personal information held by the MSC including a general account of our uses and disclosures;
    - how an individual can gain access to his or her personal information;
    - how to comment, complain or inquire about privacy issues; and,
    - brochures or other information that explain MSC’s policies, standards or codes for privacy and confidentiality.

The MSC will ensure that policies and procedures are understandable and easily accessible.

9. Individual Access
Upon request, the MSC will inform a client of the existence, use and disclosure of their personal information. The individual will be given access to that information, will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. A response to requests will be provided as soon as possible but no later than 30 days after the initial written

request is received.

In certain situations, the MSC may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement will be limited and specific. The reasons for denying access will be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

10. Challenging Compliance

Any individual (staff, client, volunteer, etc) is able to launch a challenge concerning compliance with the above principles to the Privacy Officer. Upon a challenge, the MSC will:

- have available simple and easily accessible complaint procedures (see Client Feedback Policy);
- inform complainants of avenues of recourse;
- investigate all complaints received;
- investigate and remedy any breach of information with the client's best interest in mind;
- take appropriate measures to correct information handling practices and procedures; and
- record the date a complaint is received and the nature of the complaint.

The Privacy Officer will review all feedback, make changes to the policy as needed and ensure feedback response meets legislative rights and timeliness. The Officer will notify the Privacy Commissioner as necessary.

References:

PolPro-A-RulesCon-2-2 Disclosure Policy
PolPro-A-RulesCon-3-1 Code of Ethical Conduct
PolPro-ORG-GOV-2-4 Conflict of Interest Policy
PolPro-OP-IT-1-1 Information Technology Acceptable Usage
PolPro-O-Fin-14 File Retention, Destruction & Security Policy
Client Bill of Rights & Responsibilities – Home Support
Client Bill of Rights & Responsibilities – Employment & Literacy Services
Access to Client Records Procedure
HS Procedures related to privacy and confidentiality
ES/LS Procedures related to privacy and confidentiality