Privacy Policy

Momentum is committed to the principles of public accountability and personal privacy. In our day-to-day activities, we collect important personal information about prospective, current and past participants, employees, members, donors and volunteers in order to make decisions about admission, evaluation of performance and suitability of position. It is our policy to control the collection, use and disclosure of personal information in accordance with the Fair Information Principles, The Alberta Personal Information Protection Act, The Freedom of Information and Protection of Privacy Act, The Personal Information Protection and Electronic Documents Act of Canada and other substantially similar and applicable privacy legislation. The Momentum Privacy Policy will be reviewed every five years to ensure its relevance and that it remains current with changing technologies, laws and the evolving needs of Momentum, its prospective, current and past participants, members, employees, volunteers and donors.

Introduction

At Momentum respecting privacy and personal information is an important part of our commitment to our past and current participants, members, employees, volunteers and donors. Therefore, we have created a privacy policy to ensure that we retain, use and disclose information in accordance with principles and guidelines consistent with the provisions of The Alberta Personal Protection Act, The Freedom of Information and Protection of Privacy Act, Personal Information Protection and Electronic Documents Act Canada ("PIPEDA") and other substantially similar and applicable privacy legislation. This policy has been developed to be consistent with our organization's mission, vision and values.

The ten Fair Information Principles establishes rules for the management of personal information by organizations involved in commercial activities and the collection of different types of personal information. The main objective of the principles is to strike a balance between an individual's right to the protection of personal information and the need of organizations to obtain and handle such personal information for legitimate business purposes.

Organizations that are within the scope of current and applicable privacy legislation must obtain an individual's consent when they collect, use or disclose personal information. The individual from which the information is collected is also able to challenge its accuracy, if need be. The purpose for which personal information is collected must be explained by the organization at or before the time information is collected. Momentum is responsible for the protection of personal information that it retains and the management of sensitive information internally and externally. An explanation of important privacy terminology is found in appendix a of the privacy policy.

The Ten Principles of Fair Information

1. **Accountability**: Momentum is responsible for personal information under its control and has designated individuals who are accountable for the organization's compliance with the fair information principles, Alberta's Personal Information Protection Act and other current applicable privacy legislation.

2. **Identifying Purpose**: The purpose for which personal information is collected shall be identified by Momentum during to or prior to the time information is collected. Personal information will not be used for any other purpose than that for which it has been designated.

3. **Consent**: Knowledge and consent of the individual is required for the collection, use or disclosure of personal information.

4. **Limiting Collection**: Collection shall be limited to personal information that is necessary for the purposes identified by Momentum.

5. **Limiting Use**: Disclosure and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with consent or as required by law.

6. **Accuracy**: Personal information shall be accurate, complete and up to date as necessary for the purpose for which it is to be used.

7. **Safeguards**: Personal information is protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**: Momentum shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information.

10. **Challenging Compliance**: An individual is able to address a challenge by making an inquiry with the Operations Manager for compliance with privacy principles.

The ten principles of fair information and privacy are all interconnected to help create a culture of trust and accountability at Momentum. We are proud of the initiatives we have taken to protect privacy.

Scope and Application of Privacy Policy

Protecting the privacy of each individual from whom we collect personal information from is important to Momentum. The ten principles of fair information and privacy create the foundation of our privacy policy. Each principle must be read in conjunction with the following commentary.

The scope and application of the Momentum Privacy Policy is as follows:

- The Momentum privacy policy applies to personal information that we collect in our day-to-day process that allows our organization to operate, thrive and meet the needs of the community we serve.
- The Momentum Privacy Policy applies to the management of personal information in any form whether oral, electronic or written.
- The application of the Momentum Privacy Policy is subject to the requirements and provisions of Alberta Personal Information Protection Act, the regulations enacted hereunder and any other applicable and substantially similar legislation, regulation, court order, or other lawful authority.
- Momentum is guided by the standard of what is considered reasonable in appropriate circumstances. The standard to be applied under this privacy policy in determining whether the issue or matter is reasonable or unreasonable, or it has been carried out in a reasonable manner under appropriate circumstances depending upon the specific situation and/or circumstances.
- Momentum must develop and follow policies and practices that are reasonable for our organization to meet its obligations under current privacy legislation.

Principle 1: Accountability

Momentum is responsible for personal information under its control and designates the Operations Manager to be accountable for Momentum's compliance with the principles of fair information and respond to complaints, inquiries, and systemic challenges. An individual is able to make a complaint to the Operations Manager about our policies and practices relating to the management of personal information.

1.1 Responsibility for compliance with the provisions of Momentum's Privacy Policy rests with the Operations Manager. Other individuals have also been designated to act on behalf of the Operations Manager or take responsibility for the day-to-day collection, use and disclosure of personal information.

1.2 Momentum is responsible for all personal information that we collect and is in our possession or custody. Momentum will use all means reasonable to ensure that personal information in the custody of third parties have a comparable level of protection and security.

1.3 Momentum shall develop and implement policies and procedures to give effect to our privacy policy, including:

1. Implementing procedures to protect personal information and to oversee Momentum's compliance with the Privacy Policy;

2. Establishing clear and easy to follow procedures on how to respond to access and disclosure of records;
3. Developing information materials to explain Momentum's policies and procedures.

1.4 Momentum shall implement a "delegation instrument" with which it will decentralize duties and responsibilities among all employees concerning the collection, use and disclosure of personal information. The delegation instrument is found in appendix b of the privacy policy.

Principle 2: Identifying Purpose

It is the policy of Momentum that the purpose for which personal information is collected shall be identified by the Operations Manager and various program staff at or before the time the information is collected. The knowledge and consent of program staff and participants are required for the collection, use or disclosure of personal information.

2.1 Momentum collects information only for the following purposes:

1. To determine suitability of an applicant to one of our community economic development and volunteer programs;
2. To evaluate performance or suitability of employment, volunteer and participant position;
3. To understand and respond to our prospective, current and past participants, members, employees, volunteers and donor's needs, concerns, or opinions;
4. To meet legal and regulatory requirements; and
5. To fundraise.

2.2 Momentum shall specify orally, electronically or in writing the identified purposes to the prospective, current or past participants, members, employees, volunteers and donors at or before the time personal information is collected. However, upon request an individual has the legal right to access their personal information to view or correct the accuracy of their personal file.

2.3 When personal information that has been collected is to be used or disclosed for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is permitted or required by law, the consent of the prospective, current and past participant, member, employee, volunteer and donor will be required before the personal information will be used or disclosed for the new purpose.

Principle 3: Obtaining Consent for Collection, Use, or Disclosure of Personal Information

The knowledge and consent of the prospective, current and past participants, members, employees, volunteers and donors are required for the collection, use or disclosure of personal information, except where inappropriate.

3.1 In obtaining consent, Momentum shall use reasonable efforts to ensure that prospective, current and past participants, members, employees, volunteers and donors are advised of the identified purposes for which personal information will be used or disclosed. The purpose for

which personal information is collected, used or disclosed shall be stated in a manner that can be reasonably understood by the applicant, employee, volunteer and/or donor.

3.2 The financial contribution of an individual, the acceptance of participating in one of our programs, or acceptance of employment or benefits by an employee, constitutes implied consent for Momentum to collect, use and disclose personal information for the identified purposes.

3.3 Prospective, current and past participants, members, employees, volunteers and donors may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The above mentioned may contact Momentum for more information regarding the implications of withdrawing consent.

3.4 Generally, Momentum shall seek consent to use and disclose personal information at the same time it collects the information. However, Momentum may seek consent to use and disclose personal information after it has been collected, but before it is used or disclosed for a new purpose.

3.5 In certain circumstances personal information can be collected, used or disclosed without the knowledge and consent of the individual. For example:

1. If it is clearly in the interests of the individual and consent cannot be obtained in a timely way, such as when the individual is seriously ill or mentally incapacitated.
2. If there is such an emergency where the life, health or security of an individual is threatened; or if disclosure of information is necessary to comply with the law.

Principle 4: Limiting Collection of Personal Information

Momentum shall limit the collection of personal information to that which is necessary for the purposes identified by Momentum. Momentum shall collect personal information by fair and lawful means.

4.1 Momentum collects personal information primarily from prospective, current and past participants, members, employees, volunteers and donors.

4.2 Momentum may also collect personal information from other sources including employers or personal references that present that they have the right to disclose the information with consent.

4.3 Momentum shall not collect personal employee information about an individual unless:

1. The collection is reasonable for the purpose for which it is being collected;
2. The personal employee information includes only personal information that is related to the employment or volunteer work relationship of the individual.

Principle 5: Limiting Use, Disclosure, and Retention of Personal Information

It is the policy of Momentum that personal information shall not be used or disclosed for the purposes other than those for which it was collected, except with the informed consent of the individual or as required by law. Personal information without a specific purpose or that no longer fulfils its intended purpose shall be disposed of in a manner that prevents improper access, such as the shredding of paper files or deletion of electronic records.

5.1 Momentum is committed to the principle of not disclosing information to third parties other then when it is permitted or required by law.

5.2 Momentum may disclose personal information about an individual without the consent of the individual:

1. For normal employee and benefits administration;
2. When it is required or permitted by law (e.g. personal information needed for an investigation);
3. When disclosure of the information is necessary in order to respond to an emergency that threatens the life, health or security of an individual or the public; and/or;
4. The disclosure of information is necessary to determine the individual's suitability to receive an honour, award or similar benefit.

5.3 Only Momentum's employees with a need to know or who have been authorized to preview or review certain sensitive information or whose duties or services reasonably so require, are granted access to personal information about participants, members, employees, volunteers and donors.

5.4 Momentum shall implement a retention and disposition schedule of documents to ensure that documents remain relevant for the identified purposes or as required by law. Depending on the circumstances, where personal information has been used to make a decision about a prospective, current or past participant, member, employee, volunteer or donor, Momentum shall retain, for a period of time that is reasonably sufficient to allow for access by the person, either the actual information or the rationale for making the decision.

5.5 When information is no longer considered relevant for the identified purposes or required by law to be retained, such information shall be destroyed, erased, sent to the archives or made anonymous.

Principle 6: Accuracy of Personal Information

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

6.1 Personal information used by Momentum shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about a current or past participant, member, employee, volunteer or donor.

6.2 Momentum shall update personal information about prospective, current and past participants, members, employees, volunteers and donors as necessary to fulfill the identified purposes or upon notification by the individual.

Principle 7: Security Safeguards

Momentum is committed to adopting and applying appropriate technological, organizational and physical safeguards to ensure that personal information is respected and protected according to the principles of fair information and privacy. We are determined to provide security as required by the level of sensitivity of information in our custody and foster a level of trust among the employees at Momentum and our interaction with participants, volunteers, and donors.

7.1 Momentum shall use appropriate security measures to protect information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction regardless of the format in which it is held. Momentum shall use appropriate and approved methods of deleting and removing personal information and documents that are no longer considered relevant to prevent unauthorized individuals from gaining access to documents.

7.2 All of Momentum's employees who have access to sensitive personal information shall be required as a condition of employment or engagement to respect the privacy of clients and confidentiality of personal information and shall sign an agreement of privacy. Information on other practices that are important to keeping personal information secure is found in Appendix C of the privacy policy: working with confidential information.

Principle 8: Openness Concerning Policies and Procedures

Momentum shall make readily available to all individuals inquiring about our policies and guidelines specific information relating to the management of personal information upon request.

8.1 Momentum shall make available information to help prospective, current and past participants, members, employees, volunteers and donors exercise choices regarding the use of their personal information.

Principle 9: Access to Personal Information

It is the policy of Momentum that upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. Although some exceptions do apply, an individual shall also be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

9.1 Upon request, Momentum is legally responsible to assist individuals who are seeking to review the personal information in their file. Personal information shall be provided in an understandable form within a reasonable time and at a minimal or no cost to the individual.

9.2 In certain situations Momentum may not be able to provide access to all of the personal information it holds about prospective, current and past participants, members, employees, volunteers and donors. Momentum shall provide the reasons for denying access upon request.

9.3 Momentum shall provide an account of the use and disclosure of personal information and where reasonably possible shall state the source of the information. In providing an account of disclosure, Momentum shall provide a list of files and documents consulted.

9.4 In order to safeguard personal information of a prospective, current and past participants, members, employees, volunteers and donors may be required to provide sufficient identification to permit Momentum to account for the existence, use and disclosure of personal information and to authorize access to the individual's file.

9.5 Momentum shall promptly correct any personal information found to be inaccurate or incomplete.

9.6 Individuals can obtain information or seek access to their individual information by contacting Momentum's Operations Manager.

Principle 10: Challenging Compliance

Prospective, current and past participants, members, employees, volunteers and donors shall be able to challenge the compliance with the above principles to the person accountable for Momentum's compliance with the Momentum Privacy Policy by contacting Momentum's Operations Manager.

10.1 Momentum shall maintain procedures for addressing and responding to all inquirers or complaints from prospective, current and past participant participants, members, employees, volunteers and donors about Momentum's handling of personal information.

10.2 Momentum shall inform its participants, members, employees, volunteers and donors about the existence of these procedures as well as the availability of complaint procedures.

Additional Information

For more information regarding The Momentum Privacy Policy, please contact the Operations Manager.

For a copy of The Freedom of Information and Protection of Privacy Act please visit http://www3.gov.ab.ca/foip/ or Alberta's Personal Information Protection Act please visit http://www.psp.gov.ab.ca/ For more information and background on the Information and Privacy Commissioner of Alberta or if you wish to contact the office please visit http://www.oipc.ab.ca/home/

APPENDIX A

Definitions

In this privacy policy:

"Business card information" is an individual's name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information.

"Consent" is voluntary agreement with the collection, use and disclosure of personal information. Consent can be express or implied, and provided directly by the user or through an authorized representative.

Express consent can be given orally, electronically or in writing, but is always unequivocal and does not require any inference by the individual seeking consent. Individuals are encouraged to rely primarily on electronic or written consent given the uncertainties inherent in oral consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the user.

"Collection" is the act of gathering, acquiring or obtaining personal information from any source, including from third parties, by any means. Personal information necessary to carry on the business of Momentum may be collected by Momentum employees for the suitability of position, and other functions that are necessary for the success of that program.

"Disclosure" is the action of making personal information available externally to other authorized institutions and organizations.

"Participant" is an individual who is participating or who has participated in one of our programs.

"Personal information" is information about an individual that is recorded in any form. It may include an individual's name, address, telephone number, date of birth, family status, marital status, occupation, medical and health records, assets, liabilities, income, credit rating, whether or not credit was extended or refused to the individual, credit and payment records of the individual, an individual's previous insurance experience including claims history, and an individual's driving record.

"Recorded information" about an identifiable individual includes, but is not limited to:

- The individual's name, home or business address;
- The individual's race, national or ethnic origin, colour, or religious or political beliefs, or associations;
- The individual's age, sex, marital status or family status;
- An identifying number, symbol or other particular assigned to the individual;
- Information about the individual's health and health care history, including information about a physical or mental disability;
- Information about the individual's educational, financial, employment or criminal history;
- Anyone else's opinion about the individual (character profiling); and

- The individual's personal views or opinions about an individual that we have collected and retained personal information on.

"Unauthorized person" is a person who has not been given the authority and/or permission by Momentum to view certain sensitive documents. A person can be given permission (become "authorized") by Momentum to have access to and review personal information when it is necessary to fulfill his/her duties as an employee of this organization.

"Use" is the action of utilizing personal information internally within Momentum for staff to fulfill their day-to-day duties.

APPENDIX B

Delegation Instrument

Collection, Protection and Retention of Personal Information

TRANSACTION	DECISION-MAKING AUTHORITY	IMPLEMENTATION AUTHORITY
Establish manner for controlling and protecting personal information	Operations Manager	Coordinators
Ensure authorized purpose of collection	Operations Manager	Coordinators
Ensure appropriate collection of personal information	Operations Manager	Operations Manager and Coordinators
Ensure that personal information is accurate and complete	All Staff	Operations Manager and Coordinators
Ensure that appropriate retention and disposition standards are established	All Staff	Operations Manager and Coordinators
Approve or refuse correction of personal information	Operations Manager and Coordinators	Operations Manager and Coordinators
Ensure personal information is protected	All Staff	Operations Manager and Coordinators
Approve disclosure of various forms of information	Operations Manager	Operations Manager
Approve disclosure to avert or minimize danger to the health or safety of any person	Operations Manager	Operations Manager
Approve disclosure for research or statistical purposes and administration of agreements	Operations Manager	Operations Manager
Approve disclosure to a guardian of a minor	Operations Manager	Operations Manager and Coordinators
Approve disclosure of personal information so that a relative or friend of an injured, ill or deceased individual may be contacted	Operations Manager	Operations Manager and Coordinators

Right of Access to Personal Information

TRANSACTION	DECISION-MAKING AUTHORITY	IMPLEMENTATION AUTHORITY
Assist Applicant	Operations Manager and coordinators	All Staff
Create Status Record	Operations Manager	Operations Manager
Determine exceptions to the access to records	Operations Manager	Operations Manager
Receive and reply to requests	Operations Manager	Operations Manager
Approve a 30 day extension of the time limit	Operations Manager	Operations Manager
Grant or refuse access to records	Operations Manager	Operations Manager
Provide access to records when approved	Operations Manager	Operations Manager and Coordinators
Declare request completed	Operations Manager	Operations Manager

General Provisions

TRANSACTION	DECISION-MAKING AUTHORITY	IMPLEMENTATION AUTHORITY
Create a directory for alternative avenues to file a counter complaint	Operations Manager	Operations Manager
Make available a directory for alternative avenues to file a counter compliant	Operations Manager	Coordinators
Provide facilities where the public may inspect handbooks, manuals and guidelines	Operations Manager	Operations Manager
Estimate fees	Operations Manager	Operations Manager
Approve waiver of fees	Operations Manager	Operations Manager
Promote awareness of the 10 fair information principles	Operations Manager	Coordinators
Ensure that appropriate safeguards are installed	Operations Manager	All Staff

APPENDIX C

Working with Confidential Records

What is a confidential record?

A confidential record contains information that for any one of a number of reasons should only be disclosed to specific people or groups. The information will either be recorded personal information about an identifiable person, member, employee, past and/or current participant, volunteer or donor relating to the day-to-day processes of the organization or a third party. However, it does not include publicly accessible information such as business card information, business contacts or program descriptions. The Momentum staff are obliged to fulfill their responsibility to secure sensitive information as well as protect and respect the right to privacy of current and past participants, members, volunteers, donors and other staff members. Momentum supports a community-inspired vision where individuals pursue initiatives of change within an environment that recognizes and protects the rights of an individual to have his or her personal information protected.

The access to records could encompass issues from a request to review personal files and e-mail massages to character profile assessments used to determine suitability for the program. When working with confidential documents, it is imperative that no unauthorized persons have access to them. Some methods for ensuring this are:

- Ensure that no unauthorized persons can read your computer screen;
- Have a secure password to access your computer and;
- Place working copies of confidential documents out of sight of the general public.

The information might be considered confidential if:

- The information was supplied either explicitly or implicitly in confidence, and
- Its release could result in some harm to either the individual who supplied the information, our organization and/or a third party.

The disclosure of information might be considered harmful if disclosure could:

- Significantly damage the privacy of an individual;
- Expose the individual who supplied the information to physical, emotional or mental harm;
- Result in similar information no longer being supplied;
- Result in an unreasonable invasion of a third party's personal privacy;
- Undermine the operations of our organization or cause employees to be less frank in discussions.

Working with Confidential Records

To ensure that confidential information is not inadvertently disclosed:

- If possible, position your computer screen so no unauthorized person can read it;
- Engage a screen saver, turn off the monitor, or close down the program when you are interrupted;
- Turn off your computer when you will be away from it for a long period of time;

- Have password access to your computer and ensure your password is secure;
- Place copies of the documents in folders or envelopes, out of sight of the general public;
- Place drafts and final versions in locked file cabinets when you are not working on them for a period of time;
- Shred drafts once they are no longer useful;
- Delete drafts from your computer once they are no longer useful;
- Transfer confidential documents to the archives when they reached the end of their retention limit.

Managing E-mails

E-mail messages are records of the organization and should be classified and converted to the storage medium most suitable for retention.

- Transitory e-mail messages may be deleted without conversion to another medium.
- E-mails are accessible under privacy legislation. To lessen the impact of requests for e-mails it's best to manage them as you create them or receive them. Any e-mail which should be filed according to your office classification requirements (i.e. have value, are not transitory in nature) should be printed out, filed as paper and deleted from the email system. Transitory e-mails should be deleted when read or sent.
- Where staff want to retain an e-mail on the system for office or business it should still be printed to a hard copy file where its not transitory in nature.

Travelling with Confidential Records

The employee is responsible for any and all documents taken off the Momentum premise however, he/she must make necessary and reasonable accommodations to ensure that privacy and confidentially are secure and protected:

- Take only what you absolutely need in either paper or electronic format;
- Carry all documents and records in a closed briefcase or carrying case;
- Keep the records with you at all time- do not leave them unattended in an unlocked office or meeting room;
- If you need to look at the records while en route, prevent others from being able to read them;
- Do not leave the records in an unlocked vehicle or on the seat where they are visible to passers-by;
- Return the records to their original secure storage place upon return;
- Notify your supervisor, the Operations Manager, department Coordinator and/or the police, if a theft occurs. If personal information is involved, notify those individuals whose personal information has been stolen, informing them of the theft and what information was taken.

Faxing Confidential Records

Ensure that you:

- Use our fax transmittal cover page with a privacy statement (a copy can be found on the Momentum internal website);
- Confirm the information being transmitted to a fax machine is in a secure location with controlled access or that the material will be secured upon arrival;

- Visually check the number displayed on the screen for accuracy before proceeding with the transmission;
- Confirm receipt of the material by calling the recipient after transmission or by having the recipient call you when the fax is received, if possible;
- Notify the sender and return or destroy the information if you receive a transmission in error;
- Check the number of pages received against the number sent; and
- Locate the fax machine in a secure area with controlled access.

Destroying Confidential Documents:
All records containing confidential information will be shredded.

Storing Confidential Records:
Confidential records should be stored in a secure location to ensure that no unauthorized persons will have access to the information. Secure locations include:

- Locked filing cabinets;
- Record centre in a locked room;
- Secure server.

All confidential records shall be stored in a secure area to ensure that no unauthorized person will have access to the information. Confidential records and documents will be stored in locked filing cabinets, in a locked and secure room and all necessary technological safeguards will be taken to ensure that the necessary and appropriate provisions protect privacy.