YMCAs across Southwestern Ontario **POLICY**			
Function:	Governance	**Policy #:**	GV 01.11
Section:	Governance	**Status:**	Published
Subject:	**Confidentiality and Privacy**	**Status Date:**	2015-05-21
Issued to:	All manual holders	**Effective Date:**	2013-06-14
Approved by:	Board of Directors, recommended by Executive Committee	**Next Review Date:**	2016-06-30

1.0 POLICY

1.01 The association and its employees and volunteers will take all reasonable steps to maintain the confidentiality of all confidential business information and personal information.

1.02 The association and its employees and volunteers will respect and protect the privacy of personal information. To achieve this, the association will comply with the ten privacy principles required by the Personal Information Protection and Electronic Documents Act (PIPEDA). The ten principles are:

1. Accountability
2. Identifying Purpose
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

Further elaboration of these principles is set out in Attachment A.

The association will maintain a privacy policy for distribution to customers and other interested parties, and will post this policy on its website. This is set out in Attachment B.

1.03 The association will publish its policy about the collection, use and disclosure of personal information belonging to members, participants, customers, suppliers and members of the general public, including:

a) Personal information collected and used via any association process including membership records, cookies, customer records, and supplier records.

b) The nature of the use of the information and limitations placed by the association on the use of the information.

c) The personal information disclosure practices of the association including any restrictions placed on that disclosure.

d) The limitations in time of holding personal information collected and used by the association including the association's commitment to destroying unneeded information.

e) The process by which individuals may access their personal information.

1.04 The association will maintain high standards of physical and electronic security wherever personal information is being handled, including:

a) Electronic records of personal and confidential business information are subject to limited access by authorized personnel. All files containing personal information will be protected by password.

b) Physical records of personal information will be kept in locked cabinets or secure rooms and accessible only by authorized personnel.

c) In compliance with Canada's Anti-Spam Legislation, explicit permission will be sought prior to sending commercial electronic messages, unsubscribe features will be available and email address lists will be actively managed and maintained.

1.05 The association will establish a Privacy Officer whose name and contact information will form an integral part of the privacy policy. All requests for access to personal information and all contact with the Privacy Commissioner of Canada will go through the Privacy Officer.

1.06 Personal information collected, used or disclosed related to employees will be subject to the same care and conditions as outlined for other personal information and will be supported by an internal policy on the care and access to employee personal information. This policy will include:

a) Details about the information created, collected, used and disclosed, the purpose and limitations of the use of the information.

b) The employee's right to access and correct their personal information.

c) Processes related to the access and correction of employee personal information.

2.0 PURPOSE

2.01 The purpose of this policy encompasses the elements necessary for association compliance with privacy legislation, principles and practice.

3.0 SCOPE

3.01 This policy applies to all association employees and volunteers.

3.02 It is the association's intention to apply the principles and practices outlined in this policy to all contracts and other working arrangements with consultants, contractors or others providing services to the association. Compliance with the principles outlined in this policy shall be treated as essential for contract compliance.

4.0 RESPONSIBILITY

4.01 It is the responsibility of every employee to ensure that privacy of personal information is protected and respected.

4.02 It is the responsibility of the president to appoint a Privacy Officer.

4.03 It is the responsibility of the Privacy Officer to:

a) develop and maintain both internal and external privacy policies,

b) ensure that systems and processes are in place to support the policies,

c) act as an expert resource on privacy within the association, and

d) act as a point of contact on privacy issues.

5.0 DEFINITIONS

5.01 "***PIPEDA***" is the Personal Information Protection and Electronic Documents Act, the Canadian law governing the commercial collection, use and disclosure of personal information.

5.02 "***Personal Information***" refers to all information related to a unique individual including name and contact information, identification numbers or codes, and sensitive personal information.

5.03 "***Cookies***" refers to log files planted in an individual's computer hard drive to record and save that personal information about the individual's location and preferences that it will need to use in future contacts.

5.04 "***Privacy Commissioner of Canada***" refers to the individual who has been identified by the federal government to inform and enforce the PIPEDA legislation.

6.0 REFERENCES AND RELATED STATEMENTS OF POLICY

Type	Reference
Law, regulation, governing document	Personal Information Protection and Electronic Documents Act (PIPEDA) Canada's Anti-Spam Legislation (CASL)
Other external reference	Imagine Canada Standard A13. Privacy Policy
Policy	GV 03.06 Records Retention
Process	

7.0 APPLICATION

7.01 All employees will protect and respect confidential business and personal information by:

a) Not disclosing it inside or outside the association except as required by association policy.

b) Taking all reasonable steps to secure and protect the information. Electronic records will be subject to limited access by authorized personnel in the performance of their duties who must use passwords and other security measures. Printed records of personal information, when they are not under the control of authorized personnel, will be subject to physical protection such as locked rooms or cabinets, accessible only to authorized personnel.

c) Disclosing to individuals the reason for collecting personal information about them.

d) Destroying the information when it is no longer required. Personal information will be destroyed two years after it is no longer required. Files will be archived and then destroyed or deleted in accordance with the Records Retention Policy. Archived information is not accessed or used for operational or marketing purposes.

7.02 **Appointment of Privacy Officer**

a) The CEO will appoint a Privacy Officer for the association whose name and contact information will be publicly available as the point of contact for all inquiries or issues related to privacy of personal information.

b) The Privacy Officer is responsible for:

i. Development and maintenance of the association's privacy policies both for the public and for employee records.

ii. Thorough review of the association's collection, use and disclosure of personal information to ensure that only required information is dealt with.

iii. Communication of the privacy policy for the public to the public and to all employees, including necessary employee training.

iv. Communication of the privacy policy for employee information to all employees, including necessary management training.

v. Acting as an expert resource for the association on matters relating to privacy of personal information.

vi. Ensuring that the association's systems and procedures meet all legal compliance requirements and are a standard of excellence for respect of personal information.

vii. Documenting and analyzing all complaints regarding the use, retention or disclosure of personal information.

viii. Instituting changes to the policy and related procedures deemed necessary in order to respect the principles of this policy.

7.03 **Detailed Guidelines**

a) Personal information may be collected without knowledge or consent only in the following circumstances:

i. In the event of an emergency that threatens the life, health or security of an individual.

ii. The information is publicly available.

b) Personal information may be disclosed without knowledge or consent only in the following circumstances:

i. In the event of an emergency that threatens the life, health or security of an individual.

ii. To a lawyer representing the association.

iii. To collect a debt owed to the association by the individual.

iv. If required by law.

v. The information is publicly available.

vi. For other circumstances listed in subsection 7(3) of PIPEDA.

c) Requests from an individual to provide information about their personal information being collected, used or disclosed by the association will be answered within 5 business days. The association will not charge a fee for this service.

d) If an individual withdraws consent for the use of personal information, the Privacy Officer will take all necessary steps to cease the association's use of the information within 30 days.

e) Systems will be established and maintained to actively manage e-mail lists, ensuring that commercial electronic messages are only sent to individuals who have provided explicit consent and that unsubscribe features are available and functioning as intended.

8.0 ATTACHMENTS

8.01 Appendix A – 10 Principles for the Protection of Personal Information

8.02 Appendix B – YMCA Privacy Statement

Review & Approval Record

This policy is to be reviewed at least:

Document all reviews here prior to updating Next Review Date for a Policy

Date	Reviewed by	Approved by
2014-10-25	Executive Committee	Board of Directors

Revision Control

Document all revisions here prior to issuing an updated Policy

Date	Revision
2013-07-08	Reformatted
2014-06-20	Updates to reflect CASL
2014-06-20	Updates to the Privacy Statement (Appendix B) to reflect CASL, YASWO merger, and new e-mail and web addresses
2014-07-04	Approved by Executive Committee
2014-08-12	Reference to future Communications policy and YMCA Canada photo release form added.
2015-05-21	Reformatted using new template

Appendix A – GV 1.11A

Ten Principles for the Protection of Personal Information

These 10 principles are summarized from a Model Code for the Protection of Personal Information in the National Standard of Canada, based on Schedule 1 of the PIPEDA legislation. More explicit information can be obtained by referring directly to the Schedule.

Principle 1 – Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance. Their identity should be made known upon request. The individual bears accountability for compliance regardless of who may perform related day-to-day processes. The organization is responsible for information transferred to a third party for processing and should take steps to provide a comparable level of protection of the information from that third party.

Principle 2 – Identifying Purposes

The purposes for which an organization is collecting personal information should be identified and documented at or before the time of collection. These purposes should be specified to the individual at or before the time of collection, either verbally or in writing. Care should be taken not to collect information that isn't strictly needed. Should a new purpose arise after this, the consent of the individual is again required before it can be used, unless the use is required by law.

Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where that is inappropriate. In certain circumstances, such as when medical, legal or security reasons make it impossible, personal information can be collected, used or disclosed without the knowledge or consent of the individual. An organization should not, as a condition of sale of a product or service, require consent of other uses of the information beyond that required to provide the product or service. In obtaining consent, the reasonable expectations of the individual are also relevant, as for example, an individual should reasonably expect a magazine to contact them for subscription renewals. Consent should not be obtained through any form of deception. An individual may withdraw their consent at any time subject to legal or contractual restrictions and reasonable notice.

Principle 4 – Limiting Collection

The collection of personal information should be limited to that which is necessary for the purposes identified by the organization. Information should not be collected indiscriminately. Information should not be collected illegally.

Principle 5 – Limiting Use, Disclosure and Retention

Personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information should be retained only as long as necessary for the fulfilment of those purposes. Organizations should develop documented guidelines for the retention periods for personal information. After the retention period is up, personal information no longer required should be destroyed, erased or made anonymous.

Principle 6 – Accuracy

Personal information should be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Unless it is required for the original purpose, an organization should not routinely update personal information.

Principle 7 – Safeguards

Personal information should be protected by security safeguards appropriate to the sensitivity of the information. Safeguards against loss, theft, and unauthorized access, copying, use or modification should all be addressed, including physical measures (e.g. locks, restricted access areas), organizational measures (e.g. security clearances, authorization processes) and technological measures (e.g. passwords, encryption). The nature of the safeguards should vary with the level of sensitivity of the information. Employees should be made aware of the importance of maintaining confidentiality of personal information. Care should be used in the disposal or destruction of personal information.

Principle 8 – Openness

An organization should make readily available to individuals its policies and practices relating to the management of personal information. This should include the name or title and address of the organization's Privacy Officer, how to gain access to personal information held by the association, a description of the type of information held and details of what information is made available to related organizations and why.

Principle 9 – Individual Access

Upon request, an individual should be informed of the existence, use and disclosure of his or her personal information and given access to it, within a reasonable timeframe and at limited or no cost to the individual. An individual should be able to challenge the accuracy and completeness of the information and have it amended. Under certain limited circumstances (cost, references to other's personal information, legal, security, competitive proprietary, subject to litigation or client privilege) an organization may not be able to provide the information, but these situations should be limited and specific. An organization holding sensitive medical information may choose to make it available through a medical practitioner. It is fair for an organization to require specific personal information to validate a person's identity before disclosing. Organizations should be able to provide a list of other organizations to which it has disclosed personal information.

Principle 10 – Challenging Compliance

An individual should be able to address a challenge concerning compliance with the above principles to the Privacy Officer of the organization. Principles and procedures related to this principle should be in place, and the organization should be prepared to explain these to individuals. Complaints should be documented, investigated and responded to within a reasonable period.

Appendix B – GV 1.11B

Privacy Statement for Customers, Participants and Other External Stakeholders

Privacy Statement

The YMCA is committed to protecting your right to privacy. The personal information you share with the YMCA will be used to support the work of the YMCAs across Southwestern Ontario and the Chatham-Kent Family Y.M.C.A. Foundation. We protect your personal information and adhere to all legislative requirements with respect to protecting privacy.

Anonymous Access

You can access our website home page and browse our site without disclosing your personal data. The YMCA may use cookies to store and sometimes track information about your use of our website. In addition to improving the general layout of the website, cookies allow us to customize our website to each visitor's individual preferences. Although most web browsers automatically accept cookies, you can usually change your browser to prevent you from receiving cookies or to notify you whenever you are sent a cookie so that you may decide whether or not to accept it. If you decide not to accept a cookie, you can still enjoy all of the features of our website.

In order to make your web site experience more informational and resourceful, our web site may also provide links to third party sites. The YMCA assumes no responsibility for the information practices of sites you are able to access through our site. We encourage visitors to review each site's privacy policy before disclosing any personally identifiable information.

Your Choice

We collect personal data when you volunteer to provide it online, or when you access our programs and services, in order to better meet your program, service, and information needs and further the charitable work of the YMCA. These purposes include:

- Volunteer development
- Relationship development and opportunities to give
- Safety and security
- Program and service registration and development
- Employment relations
- Legal, regulatory and contractual requirements
- Supporting participants' needs and eligibility for other services in the community

We also use and disclose data, which does not identify individuals, within our association or within YMCA Canada for statistical purposes to develop and enhance YMCA programs and services.

If you supply us with your email or mailing address, you may receive mailings from us with important information about the YMCA program or service in which you are registered.

You may also receive periodic mailings from us with information about other YMCA programs and services that may interest and benefit you or surveys requesting your input to improve YMCA programs or services. If you do not wish to receive these other mailings, please use the unsubscribe link built into those e-mails or contact YMCA Membership Services at 1-800-804-7415 or (519) 336-9622 (Sarnia).

If you wish to reverse your previous opt-out choice and receive information about other YMCA programs and services, please send an email with your request to admin@ymcaswo.ca, or contact YMCA Membership Services at 1-800-804-7415 or (519) 336-9622 (Sarnia).

Information Sharing

We do not sell or rent personal information we collect.

We will not disclose your personal information to anyone else without your prior knowledge or consent, except when required by a government body or agency, or as permitted by law.

Children's Privacy

The YMCA, in keeping with our Mission and Vision, believes in the development of healthy, confident children.

For children under 12 years of age, we will obtain permission from a parent or legal guardian to collect and use personally identifiable information about a child.

Confidentiality / Security

The YMCA maintains physical, electronic, and administrative safeguards that are appropriate to the type of personal information we obtain from you.

YMCA staff and volunteers having access to personal data are trained and required to respect the confidentiality of personal data and handle personal data responsibly.

Privacy Questions

If you are aware of any inaccuracy or changes in your personal information that we hold about you, please contact a YMCA staff at your local YMCA.

If you have an inquiry about YMCA privacy practices, please contact a senior staff at your local YMCA or contact YMCA Association Services at:

1015 Finch Drive, Sarnia, ON N7S 6G5
Tel: 519-336-9622 or 1-800-804-7415
Fax: 519-336-6676
Email: ymca@ymcaswo.ca

If you have a complaint or concern about YMCA information handling practices, we encourage you to talk to us.

In most cases, discussing your concern with a General Manager for your YMCA program or service will address your concern.

If the problem is not resolved to your satisfaction, you can contact Association Services (see contact information above). You will be asked to provide the following information in writing:

- Your name, address, or fax number where you prefer to be reached;
- Nature of your complaint, relevant details, and what you would like us to do;
- Name of the YMCA staff with whom you have already discussed the issue.

The YMCA will investigate and assist with resolving your concern.

Ongoing Relevancy

The YMCA regularly reviews its policies and procedures to ensure that we remain current with changing laws and evolving public expectations. The YMCA may at any time, without notice to you and in its sole discretion, amend this policy from time to time. The most current version of this Privacy Policy is found on the YMCA's web site. Please review this policy periodically.