



PRIVACY POLICY

Policy Number:

Date Approved: June 24, 2009

Approved By: Board of Directors

Purpose

The purpose of this policy is to protect the privacy of individuals with respect to personal information held by the Host Society, set out how the Host Society collects and uses that personal information, and to outline a process for responding to privacy-related inquiries and complaints.

Policy Statement

The Host Society is committed to the protection of personal information for its athletes, sponsors, participants, volunteers and employees.

Context

In planning and delivering the 2011 Canada Winter Games, the Host Society will be involved in the collection, use and/or disclosure of personal information related to activities like:

- Creating and maintaining medical records for athletes during Games-time
- Administering the application process for employment or volunteer consideration
- Hiring employees, and administering the payroll and benefits program
- Managing employees, specifically conducting performance management evaluations
- Processing accreditations for the Games
- Facilitating communication, via e-newsletters as an example
- Administering participation in contests
- Granting access to certain special features of the Host Society's website

The Host Society is subject to the *Personal Information Protection and Electronic Documents Act (2001)*-PIPEDA, and as such, must comply with its directives and guidelines.

As part of the Multi-Party Agreement (MPA) between the Host Society, its government partners and the Canada Games Council, the Host Society must develop a privacy policy.

Privacy protection in Canada focuses on safeguarding personal information. Drawing upon generally accepted fair information practices, the legislation seeks to allow individuals to decide for themselves, to the greatest

extent possible, with whom they will share their personal information, for what purposes and under what circumstances.¹

Brief History of Privacy Legislation:

- The Organization for Economic Co-operation and Development (OECD) released *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Information* in order to harmonize the data protection practices of member countries by means of minimum standards for handling personal information in 1980. These guidelines have served as the foundation for legislated fair information practices. When Canada affirmed its commitment to the OECD Guidelines in 1984, it applied only to the actions of governments and government agencies.²
- In response to the lack of national data protection standards in Canada, a committee of consumer, business, government, labour and professional representatives developed, with support from the Canadian Standards Association (CSA), a set of privacy protection principles that in 1996 were approved as a national standard by the Standards Council of Canada. The *Model Code for the Protection of Personal Information* was designed to serve as a model that could be adopted by businesses and modified to suit their particular circumstances.³
- In January 1998, Industry Canada and the Department of Justice released a discussion paper, in which it was noted that “legislation that establishes a set of common rules for the protection of personal information will help to build consumer confidence and create a level playing field [so that] the misuse of personal information cannot result in a competitive advantage.” As a result, Bill C-6, the *Personal Information Protection and Electronic Documents Act- PIPEDA* was enacted in 2001, to set out ground rules for the management of personal information. It balances an individual's right to the privacy of personal information with the need of organizations to collect, use and/or disclose personal information for legitimate business purposes.⁴
- In addition to federal legislation, every province and territory has privacy legislation governing the collection, use and disclosure of personal information held by government agencies. Nova Scotia was the first province in Canada to enact a *Freedom of Information Act* in 1977, and since that time, other jurisdictions in Canada have followed suit. The *Act* was replaced in 1993 by the *Freedom of Information and Protection of Privacy Act*. “Pursuant to the *Acts*, all public bodies, municipalities and local public bodies are obliged to adopt a policy of accountability, openness and transparency and to provide a right of access to information with limited exceptions. They are also obliged to ensure the protection of individuals' personal privacy.”⁵
- “The Municipal Government Act (MGA) which provides authority for most of the activities and operations of municipal governments in Nova Scotia, also contains provisions relating to freedom of information and protection of privacy (FOIPOP)”.⁶

¹ Library of Parliament (2008) *Canada's Federal Privacy Laws*
<http://www.parl.gc.ca/information/library/PRBpubs/prb0744-e.htm>

² Ibid.

³ Ibid

⁴ Ibid

⁵ The Nova Scotia Freedom of Information and Protection of Privacy Office (2006) <http://www.foipop.ns.ca/>

⁶ Halifax Regional Municipality (2004-2009) *What is FOIPOP?* <http://www.halifax.ca/irm/what.html>

PIPEDA requires organizations to “obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.”⁷

Scope

This policy applies to athletes, participants, sponsors, volunteers, and employees of the Host Society. The policy addresses the way the Host Society collects, uses, discloses and protects personal information, and a person's right to have access to their personal information.

Definitions

Consent: voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Disclosure: making personal information available to others outside the organization.

Host Society Workplace: refers to a physical location whereby the employee or volunteer has approval from the CEO Office to conduct Host Society business. Workplaces may include sport venues, Host Society offices, volunteer centre, etc.

Personal Information: includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- Age, name, address, personal telephone number, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, or disciplinary actions; and,
- employee files, credit records, loan records, medical records, intentions (for example, to acquire goods or services or change jobs).
- Personal information **does not include** the name, title or business address or telephone number of an employee of an organization.

Privacy Coordinator: staff position responsible for coordinating implementation of the Privacy Policy, including responding to inquiries and complaints on behalf of the Host Society and providing regular updates to the CEO.

Privacy Risk Assessment (PRA): a process to determine the impacts of an initiative, policy, or service on an individual's privacy and outline a way to reduce or mitigate the areas of risk.

⁷ Office of the Privacy Commissioner of Canada (2009) *A Guide for Businesses and Organizations- Your Privacy Responsibilities* http://www.priv.gc.ca/information/guide_e.cfm#002

Principles and Guidelines

Overall

The Host Society must analyze all personal information handling practices-- including ongoing activities and new initiatives-- using the following checklist to ensure that they meet fair information practices:

- € What personal information do we collect?
- € Why do we collect it?
- € How do we collect it?
- € What do we use it for?
- € Where do we keep it?
- € How is it secured?
- € Who has access to or uses it?
- € To whom is it disclosed?
- € When is it disposed of?

In addition, there are common principles associated with privacy, developed by the Canadian Standards Association and outlined in PIPEDA. The Host Society's Privacy policy includes these principles:

Principle 1 – Accountability

The Host Society is responsible for personal information under its control and for establishing and implementing policies and practices for the appropriate collection, retention and use of the personal information. Furthermore, the Host Society is also responsible for information that has been transferred to a third party for processing.

Principle 2 – Identifying Purposes

The purpose(s) for which personal information is collected must be identified to the person by the Host Society before or at the time the information is collected.

Principle 3 – Consent

The knowledge and consent of the person is required for the collection, use, or disclosure of personal information, except as provided in this principle.

Principle 4 – Limiting Collection

The collection of personal information must be limited to that which is necessary for the purpose(s) identified by the Host Society. Information must be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure & Retention

Personal information must not be used or disclosed for purpose(s) other than those for which the information was collected, except with the consent of the Person or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purpose(s).

Principle 6 – Accuracy

Personal information must be as accurate, complete and up-to-date as is necessary for the purpose(s) for which it is to be used.

Principle 7 – Safeguards

Personal information must be protected by security safeguards appropriate to the sensitivity of the information.

Principle 8 – Openness

The Host Society must make readily available specific information about its policies and practices relating to the management of personal information.

Principle 9 – Access

Upon request, a person must be informed of the existence, use and disclosure of his or her personal information and must be given access to that information. A person must be able to assess the accuracy and completeness of the information and have it amended as appropriate.

Principle 10 – Challenging Compliance

A person must be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the Host Society’s compliance.

Overall Guidelines:

1. When collecting personal information, the Host Society should be able to explain the purpose(s) for which the information is being collected; the Host Society must document the purpose(s) for which personal information is collected. The Limiting Collection principle requires the Host Society to collect only that information necessary for the purpose(s) that have been identified. Identifying the purpose(s) for which personal information is collected at or before the time of collection allows the Host Society to determine the information it needs to collect and fulfill these purpose(s).
2. The identified purpose(s) should be specified at, or before the time of collection to, the person from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, pamphlet or other suitable media, for example, may give notice of the purpose(s) for which personal information is being collected.
3. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose must be identified before use. Unless the new purpose is required by law, the consent of the person is required before personal information can be used for that purpose.
4. The Host Society is responsible for personal information in its possession, custody or control, including information that has been transferred to a third party for processing. Prior to disclosing any personal information to any third party, the Host Society will use contractual or other means to provide a comparable level of protection while the personal information is in the possession, custody or control of a third party.
5. The following steps must be followed to protect personal information:
 - a. A Privacy Risk Assessment (PRA) should be conducted during the planning stages of designing a new initiative, policy or service in order to determine the impacts on an individual’s privacy and identify ways to reduce or mitigate the areas of risk. Refer to Appendix A- Privacy Risk Assessment Checklist for more details.

- b. Security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. The Host Society must protect personal information regardless of the format in which it is held.
 - i. Access to files—electronic or physical-- containing personal information must be limited to those individuals who need access for operational requirements/performance of their duties with the Host Society
 - ii. Databases and directories that contain personal information must be password-protected and/or require a user ID and password in order to access the database. Access to databases must be determined based on job/role functions and needs related to the performance of job/role-related duties with the Host Society
 - iii. Filing cabinets that contain personal information must always be kept locked
 - iv. Personal information must not be stored on USB keys/thumb drives, or other removable media
 - v. Files containing personal information must not be removed from Host Society workplaces or left unattended
 - vi. Blackberries and other personal devices that may contain personal information should be password-protected
 - vii. Disposal of records containing personal information must be carried out using only secured methods, such as shredding
 - viii. Employees and volunteers who are involved in the collection, use and/or disclosure of personal information must undergo and successfully complete appropriate background checks, including the Criminal Records Check. Employees must also review and sign a confidentiality clause as part of their employment agreement with the Host Society
- c. The Host Society's Code of Conduct must include a section discussing confidentiality
- d. The Host Society must be open about its policies and practices with respect to the management of personal information. Persons must be able to acquire information about the Host Society's policies and practices without unreasonable effort. This information must be made available in a form that is generally understandable. The information made available must include:
 - i. the name or title and address of the person who is accountable for the Host Society's policies and practices and to whom complaints or inquiries can be forwarded;
 - ii. the means of gaining access to personal information held by the Host Society;
 - iii. a description of the type of personal information held by the Host Society, including a general account of its use;
 - iv. a copy of any brochures or other information that explain the Host Society's policies, standards or codes; and
 - v. what specific personal information is made available to organizations related to the Host Society (e.g. committees).

6. The Host Society must adopt procedures to receive and respond to complaints or inquiries about its policies and practices relating to the handling of personal information. The objective of the complaint procedures is that they be easily accessible and simple to use. Those procedures must include:
 - a. receipt of complaints by telephone, mail, in person or by electronic mail;
 - b. recording of the complaint;
 - c. investigation of the complaint;
 - d. recording of interviews, statements, and other details of the incident;
 - e. determining a resolution;
 - f. implementing a resolution;
 - g. advising the complainant of the result of the investigation and resolution.

In addition,

- h. The Host Society must inform persons who make inquiries or lodge complaints of the existence of relevant complaint procedures.
 - i. The Host Society must investigate all complaints. If a complaint is found to be justified through either the internal or external complaint review process, the Host Society must take appropriate measures, including amending its policies and practices, if necessary.
7. The Host Society will implement the following steps to respond to inquiries and complaints:
 - a. The inquiry or complaint must be made in writing, using the Request Form in Appendix B.
 - b. Completed request forms must be submitted in a timely manner to the Host Society's Privacy Coordinator (Director of Human Resources and Volunteers)
 - c. The Privacy Coordinator will review and investigate the request or complaint, and provide a written response within 30 days.
 - d. There are limitations to responding to inquiries and complaints, specifically if in responding to the request the following may occur:
 - i. reveal personal information about a third party, or
 - ii. breach a solicitor-person privilege, or
 - iii. potentially threaten the life or security of another individual, or
 - iv. disclose personal information collected to investigate a breach of an agreement or contravention of law, or
 - v. reveal information generated in the course of a dispute resolution process.
8. The Host Society must communicate and educate athletes, volunteers and employees about the Privacy policy. Tools such as checklists may be used to help Host Society employees and volunteers understand their accountabilities associated with the Policy.

Guidelines related to Consent

1. Consent is required for the collection of personal information and the subsequent use or disclosure of this information.

2. The Host Society must obtain consent for the use or disclosure of the information at the time of collection.
3. The Host Society must make a reasonable effort to ensure that the person is advised of the purpose(s) for which the personal information will be used. To make the consent meaningful, the purpose(s) must be stated in such a manner that the individual can reasonably understand how the personal information will be used or disclosed.
4. Consent can be given by an authorized representative (such as a legal guardian or a person having power of attorney).
5. The Host Society must not, as a condition of the supply of a service or product, require a person to consent to the collection, use, or disclosure of personal information beyond that required to fulfill the explicitly specified purpose(s). The Host Society must explain to the person the personal information requirements that are related to the product or service. In so doing, the Host Society provides a specified, explicit and legitimate purpose. The Host Society can then refuse to deal with a person who will not consent to the collection, use and disclosure of the personal information for the specified, explicit and legitimate purpose.
6. The form of the consent sought by the Host Society may vary, depending upon the circumstances and the type of personal information. In determining the form of consent to use, the Host Society must take into account the sensitivity of the personal information. People can give consent in many ways. For example:
 - an application form may be used to seek consent, collect personal information and inform the Person of the use that will be made of the personal information. By completing and signing the form, the Person is giving consent to the collection and the specified uses;
 - a check-off box may be used to allow persons to request that certain or all personal information not be given to third parties. Persons who do not check the box are assumed to consent to the transfer of this personal information to third parties for specified purposes;
 - consent may be given orally when personal information is collected over the telephone, provided that the Host Society reasonably verifies the identity of the person giving consent over the telephone;
 - consent may be given at the time that the person requests or uses a product or service; or
 - consent may be given electronically over the Internet or by other electronic means, if the Persons can be reliably identified as the source of such consent.
7. A person may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Host Society must inform the person of the implications of such withdrawal. Absent any such withdrawal, consent is valid for the length of time needed to achieve the identified purposes.

8. Consent is not required for the collection, use and disclosure of personal information for legal or security reasons such as the collection of personal information for the detection and prevention of fraud or compliance with subpoenas, search warrants and other court, regulatory or government orders, where obtaining consent might defeat the purpose of collecting the information.

Guidelines Regarding the Collection of Personal Information:

1. The Host Society must not collect personal information indiscriminately. Both the amount and the type of information collected must be limited to that which is necessary to fulfill the purpose(s) identified.
2. The Host Society may obtain personal information from people through hard copy, electronic or other means, and sources including but not limited to credit bureaus, third party websites or other third parties who represent that they have the right to disclose the information.
3. The Host Society must collect personal information from third parties only with the consent of the person concerned, unless the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way. The Host Society must specify the type of information collected as part of its information-handling policies and practices in accordance with the Openness principle.
4. The requirement that personal information be collected by fair and lawful means is intended to prevent the Host Society from collecting information by misleading or deceiving persons about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

Guidelines Regarding the Disclosure of Personal Information:

1. There are situations specific to the Games where the Host Society will disclose personal information that is necessary in the course of organizing and conducting the Canada Winter Games. Only the personal information necessary for these purposes will be provided by the Host Society. Every such disclosure must be made subject to the protection measures specified below.
 - a. In using personal information for a new purpose, the Host Society must document this purpose.
 - b. The Host Society must, as an ongoing process, develop guidelines with respect to the retention of personal information. These guidelines will, if deemed appropriate, include minimum and maximum retention periods, subject to any legislative requirements.
 - c. Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased or made anonymous. The Host Society will, as an ongoing process, shred all paper records containing personal information, and erase in a proper fashion all computer records.

Guidelines Regarding the Accuracy of Personal Information:

1. The extent to which personal information must be accurate, complete and up-to-date will depend upon the use of information, taking into account the interests of the person. Information must be sufficiently accurate, complete and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the person.
2. The Host Society must not routinely update personal information, unless such a process is necessary to fulfill the purpose(s) for which it was collected.
3. Personal information that is used on an on going basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

Accountabilities

Board of Directors

The Board of Directors is accountable for providing oversight and guidance regarding the policy.

CEO

The CEO is accountable for:

- Ensuring the Host Society's compliance with the policy and legislation and ensuring that a process for responding to complaints is established.
- Identifying a Privacy Coordinator, to oversee the policy's implementation and respond to privacy-related concerns and inquiries.
- Reporting to the Board of Directors regarding any issues that are brought forward to the Host Society.

Privacy Coordinator

The Privacy Coordinator is accountable for:

- Responding to reports of privacy-related concerns and inquiries, following a structured, established and communicated process.
- Ensuring inquiries are responded to in a timely manner, within 30 days of the report submission.
- Identifying when a resolution to an inquiry requires a change in Host Society's policies or practices, and identifying the required changes to the CEO.
- Coordinating with appropriate resources, such as the provincial government's Office of the Ombudsman, municipal government Privacy Coordinator, federal Office of the Privacy Commissioner, or other government resources as needed.

Division Chairs

Volunteer Division Chairs are accountable for:

- Ensuring volunteers are made aware of the policy.
- Complying with the policy and its guidelines.
- Supporting the policy's implementation within their respective areas.

Divisional Directors and Managers

Divisional Directors and Managers are accountable for:

- Ensuring employees are made aware of the policy
- Complying with the policy and its guidelines
- Conducting a privacy risk assessment when designing a new policy, initiative or service offering
- Supporting the policy's implementation within their respective areas.

Employees

Employees are accountable for:

- Complying with the policy and supporting its implementation.
- Ensuring their personal information shared with the Host Society is kept up-to-date and accurate.

Volunteers

Volunteers are accountable for:

- Complying with the policy and supporting its implementation.
- Ensuring their personal information shared with the Host Society is kept up-to-date and accurate.

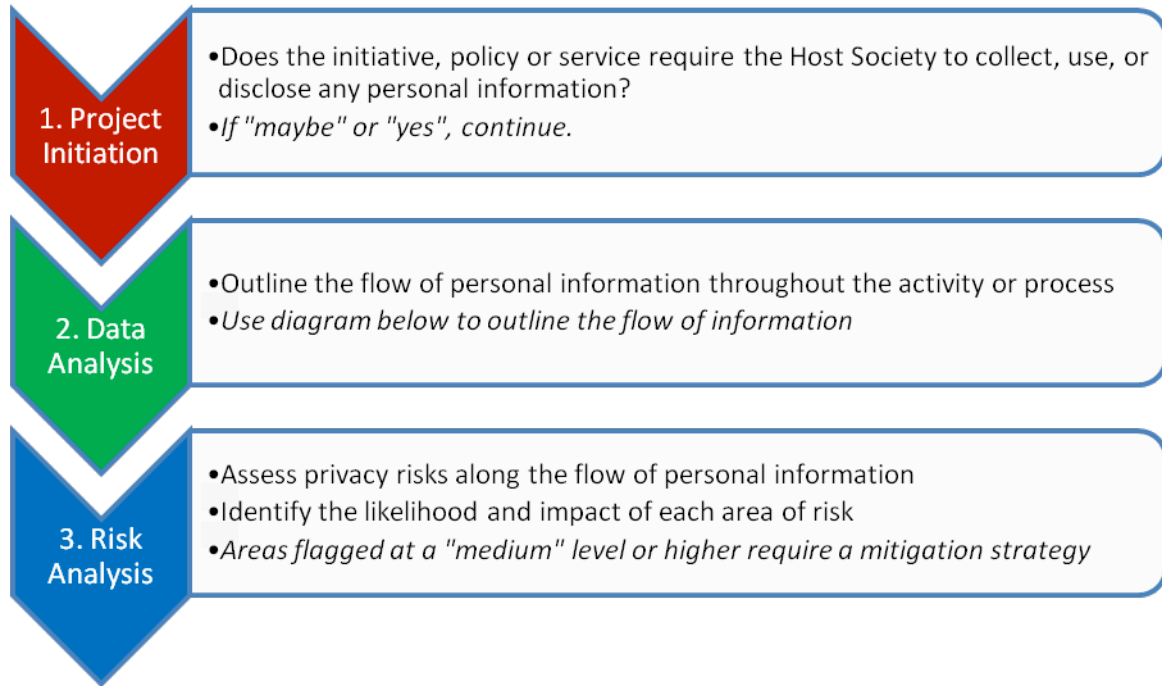
References

- Government of Canada, *Personal Information Protection and Electronic Documents Act*
<http://laws.justice.gc.ca/PDF/Statute/P/P-8.6.pdf>
- Privacy Code, 2007 Canada Winter Games
- 2011 Canada Winter Games Host Society Code of Conduct
- 2011 Canada Winter Games Host Society Website Usage/Privacy Code
- Multi-Party Agreement between the 2011 Canada Winter Games Host Society, the Government of Canada, Government of Nova Scotia, Halifax Regional Municipality and the Canada Games Council

<i>Date</i>	<i>Modified by</i>	<i>Update</i>
June 24, 2009	C.Hotton	Draft presented to BOD for approval

Appendix A- Privacy Risk Assessment Checklist

A Privacy Risk Assessment (PRA) determines the impact(s) of an initiative, policy, or service on an individual’s privacy and outlines a way to reduce or mitigate the areas of risk. The following process should be followed when completing a PRA.



Flow of Personal Information

Type of Personal Information Collected	Collected by Whom	Type/ Format of the Information	Used by Whom	Purpose of Collecting the Personal Information	Personal Information is Disclosed to Whom	How the Personal Information will be Stored/ Retained
<i>Insert comments</i>	<i>Insert comments</i>	<i>Insert comments</i>	<i>Insert comments</i>	<i>Insert comments</i>	<i>Insert comments</i>	<i>Insert comments</i>

Risk Assessment

For each area that is identified as an area of risk, please identify the likelihood/ probability of the risk as well as the impact of the risk, using the following scale: low, medium, high. Please complete the table below for each area of risk.

Area of Risk

- *Enter information/comments*

Likelihood/Probability

- *Enter level and comments*

Impact of the Risk

- *Enter level and comments*

Mitigation Strategy

- *Enter comments, outline how the risk will be mitigated*

Privacy Risk Assessment Checklist

To identify areas of risk identified through the risk assessment process, the following checklist should be used to complement the guidelines outlined in the Privacy Policy:

- € What personal information do we collect? Why do we collect it? What do we use it for? Can we define the purpose of its collection?
- € How do we collect it? What are the procedures for obtaining consent?
- € Where do we keep it? How is it secured? How do we limit the collection, use and disclosure of personal information?
- € Who has access to or uses it? What is the process for responding to inquiries or complaints?
- € To whom is it disclosed?
- € When is it disposed of?

Appendix B- Privacy Inquiry/Request Form

Date of Request:			
Your Name:			
<i>Contact Information, to send correspondence</i>			
Your email address:		Your telephone number:	
Your mailing address:			
Details of your inquiry:			
<i>€ I request access to personal information about myself as part of the Protection of Personal Information and Electronic Documents Act (PIPEDA).</i>			
Signature: _____		Date: _____	
To submit your request, please mail to: Carrie Hotton-MacDonald, Privacy Coordinator Halifax 2011 Canada Games PO Box 1749 Halifax, Nova Scotia B3J 3A5.			
<i>Please note that the Host Society's Privacy Coordinator will provide a written response to your inquiry within 30 days following receipt of your inquiry.</i>			