

Ophea Privacy Policy

Article 1 General

1.1

Purpose - The purpose of this policy is to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of the Ontario Physical and Health Education Association, herein after referred to as Ophea, to collect, use or disclose personal information.

1.2

Definitions - The following terms have these meanings in this Policy:

- a. Act - Personal Information Protection and Electronic Documents Act
- b. Commercial Activity - any particular transaction, act or conduct that is of a commercial character.
- c. Organization - includes an association, a partnership, a person, an unincorporated association, a trust, a not for profit organization, a trade union and a corporation.
- d. Personal Information - any information about an identifiable individual, but does not include business information such as an employee's name, title, business address, business email, business fax or telephone number. Personal information examples are as follows but not restricted to:
 - Name – if not public knowledge, age, gender, home address or phone number, ethnic background, family status, income
 - Evaluations, comments or disciplinary actions
 - Employee files, credit records, load records, existence of a dispute between consumer and a merchant and intentions to acquire good or services or to change jobs
 - Medical or health conditions or health services received by them, blood type
 - Religion, politics, opinions expressed by an individual or an opinion or evaluation of an individual.
- e. Personal Health Information - any health information about an identifiable individual.
- f. Representatives - Directors, officers, employees, committees, members, volunteers, contractors and other decision makers with Ophea.
- g. Individuals - prospective members, members, participants, staff and volunteers.

1.3

Application - This Policy applies to directors, officers, employees, committees, members, volunteers, contractors, and other decision makers with Ophea.

1.4

Statutory Obligations - Ophea is governed by the Personal Information Protection and Electronic Documents Act in matters involving the collection, use and disclosure of personal information.

1.5

Additional Obligations - In addition to fulfilling all requirements of the Act, Ophea and its Representatives will also fulfill the additional requirements of this Policy. Representatives of Ophea will not:

- a. Disclose personal information to a third party during any business or transaction unless such business, transaction or other interest is properly consented to in accordance with this policy;
- b. Knowingly place themselves in a position where they are under obligation to any person to disclose personal information;
- c. In the performance of their official duties, disclose personal information to family members, friends or colleagues, or to organizations in which their family members, friend or colleagues have an interest;

- d. Derive personal benefit from personal information that they have acquired during the course of fulfilling their official duties with Ophea; and
- e. Accept any gift or favour that could be construed as being given in anticipation of, or in recognition for, the disclosure of personal information.

1.6

Ruling on Policy - Except as provided in the Act, the Board of Directors of Ophea shall have the authority to interpret any provision of this Policy that is contradictory, ambiguous, or unclear.

Article 2 Accountability

2.1

Privacy Officer - Ophea shall designate an individual to oversee the implementation and monitoring of this Privacy Policy and the security of personal information.

2.2

Duties - The Privacy Officer shall:

- a. Implement procedures to protect personal information;
- b. Establish procedures to receive and respond to complaints and inquiries;
- c. Train staff and communicate to staff information about the Ophea's policies and practices; and
- d. Develop information to explain Ophea's policies and procedures to members and the public.

2.3

Staff Training - The Privacy Officer shall ensure all staff implement the proper procedures to protect personal information.

2.4

Identity - The identity of the person responsible for the Privacy Policy and his/her contact information shall be made known via Ophea's web site and will be publicly accessible.

2.5

Inquiries - The Privacy Officer shall be responsible to respond to all requests and inquiries in regards to personal information.

2.6

Principles - Ophea shall implement policies and practices to secure all personal information during collection, use and disclosure.

2.7

Disclosure to Third Parties - A contract made with a third party having access to personal information held by Ophea should include a clause that ensures the third party does not breach Ophea's privacy policies.

2.8

Information - Information shall be made available to the public via Ophea's web site explaining privacy policies and procedures.

2.9

Annual Review - This Policy shall be reviewed annually by the Privacy Officer and necessary changes shall be made to ensure the protection of personal information and compliance with the law.

Article 3 Identifying Purposes

3.1

Collection - Ophea shall only collect information reasonably necessary for the identified purposes set out in Article 3.2.

3.2

Purpose - Personal information may be collected from Individuals and used by Ophea Representatives for purposes that include, but are not limited to, the following:

- a. Name, address, phone number, cell phone number, fax number and e-mail address for the purpose of providing contact, demographic and/or service delivery information to Ophea.
- b. Credit card information for purchasing services and other resources.
- c. Banking information, social insurance number, criminal records check, resume, and beneficiaries for Ophea's payroll, company insurance and health plan.
- d. Any other information required to complete an order, evaluation, application or registration.

3.3

Identity - Ophea shall identify, in writing or communicate verbally, the purposes for which personal information is collected at or before the time of collection. The purposes will be stated in a manner that an individual can reasonably understand how the information will be used or disclosed.

3.4

Purposes not Identified - Ophea shall seek consent from individuals when personal information is used for a purpose not previously identified. This consent shall be documented as to when and how it was received.

Article 4 Consent

4.1

Consent - Ophea shall obtain consent from individuals at the time of collection prior to the use or disclosure of the information. If consent of the collection, use or disclosure was not obtained upon receipt of the information, consent shall be obtained prior to the use or disclosure of the personal information.

4.2

Lawful Means - Consent shall not be obtained by deception.

4.3

Requirement - Ophea shall not, as a condition of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfill the specified purpose.

4.4

Form - Consent may be written, oral or implied. In determining the form of consent to use, Ophea shall take into account the sensitivity of the information, as well as the individual's reasonable expectations. Individuals may consent to the collection and specified used of personal information in the following ways:

- a. By signing an application form;
- b. By checking a check off box;
- c. By providing written consent either physically or electronically;
- d. By consenting orally in person; or
- e. By consenting orally over the phone.

4.5

Withdrawal - An individual may withdraw consent to the collection, use or disclosure of personal information at any time, subject to legal or contractual restrictions, provided the individual gives one week's notice of such withdrawal. Ophea shall inform the individual of the implications of such withdrawal.

4.6

Legal Guardians - Consent shall not be obtained from individual who are minors, seriously ill, or mentally incapacitated and therefore will be obtained from a parent, legal guardian or person having power of attorney.

4.7

Exceptions for Collection - Ophea is not required to obtain consent for the collection, of personal information if:

- a. it is clearly in the individual's interests and consent is not available in a timely way;
- b. knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;
- c. the information is for journalistic, artistic or literary purposes;
- d. the information is publicly available as specified in the Act.

4.8

Exceptions for Use - Ophea may use personal information without the individual's knowledge or consent only:

- a. if Ophea has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation;
- b. for an emergency that threatens an individual's life, health or security;
- c. for statistical or scholarly study or research and Ophea must notify the Privacy Commissioner before using the information;
- d. if it is publicly available as specified in the Act;
- e. if the use is clearly in the individual's interest and consent is not available in a timely way;
or
- f. if knowledge and consent would compromise the availability or accuracy of the information and collection was required to investigate a breach of an agreement or contravention of a federal or provincial law.

4.9

Exceptions for Disclosure - Ophea may disclose personal information without the individual's knowledge or consent only:

- a. to a lawyer representing Ophea;
- b. to collect a debt the individual owes to Ophea;
- c. to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- d. to a government institution that has requested the information, identified its lawful authority, and indicated that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or that suspects that the information relates to national security or the conduct of international affairs; or is for the purpose of administering any federal or provincial law;
- e. to an investigative body named in the Act or government institution on Ophea's initiative when Ophea believes the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or suspects the information relates to national security or the conduct of international affairs;
- f. to an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law;
- g. in an emergency threatening an individual's life, health, or security and Ophea must inform the individual of the disclosure;

- h. for statistical, scholarly study or research and Ophea must notify the Privacy Commissioner before disclosing the information;
- i. to an archival institution;
- j. 20 years after the individual's death or 100 years after the record was created;
- k. if it is publicly available as specified in the regulations; or
- l. if otherwise required by law.

Article 5 Limiting Collection

5.1

Limiting Collection - Ophea shall not collect personal information indiscriminately. Information collected shall be for the purposes specified in Article 3.2.

5.2

Method of Collection - Information shall be collected by fair and lawful means.

Article 6 Limiting Use, Disclosure and Retention

6.1

Limiting Use - Personal information shall not be used or disclosed for purposes other than those for which it was collected as described in Article 3.2, except with the consent of the individual or as required by law.

6.2

Retention Periods - Personal information shall be retained for certain periods of time in accordance with the following:

- a. Employee information shall be retained for a period of seven years in accordance with Canada Customs and Revenue Agency requirements.
- b. Marketing and evaluation information shall be retained for a period of one year after compilation and analysis of collected information and destroyed thereafter.
- c. As otherwise may be stipulated in federal or provincial legislation.

6.3

Destruction of Information - Documents shall be destroyed by way of shredding and electronic files shall be deleted in their entirety.

6.4

Exception - Personal information that is used to make a decision about an individual shall be maintained for a minimum of six months of time to allow the individual access to the information after the decision has been made.

6.5

Third Parties - Information which has been consented to be disclosed to a third party shall be protected by a third party agreement to limit use and disclosure.

Article 7 Accuracy

7.1

Accuracy - Personal information shall be accurate, complete and up to date as is necessary for the purposes for which it is to be used to minimize the possibility that inappropriate information may be used to make a decision about the individual.

7.2

Update - Personal information shall only be updated if it is necessary to fulfill the purposes for which the information was collected unless the personal information is used on an ongoing basis.

7.3

Third Parties - Personal information disclosed to a third party shall be accurate and up-to-date.

Article 8 Safeguards

8.1

Safeguards - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information against loss or theft, unauthorized access, disclosure, copying, use or modification.

8.2

Sensitivity - The nature of the safeguards shall be directly related to the level of sensitivity of the personal information collected. The more sensitive the information, the higher the level of security employed.

8.3

Methods of Protection - Methods of protection and safeguards include, but are not limited to, locked filing cabinets, restricted access to offices, security clearances, need-to-know access and technological measures including the use of passwords, encryption, and firewalls.

8.4

Employees - Employees shall be made aware of the importance of maintaining personal information confidential and have been required to sign confidentiality agreements, as part of employment agreements.

8.5

Financial Information - Personal information of employees shall be secured in a locked filing cabinet and on a password protected computer accessed only by the Director of Operations and Finance Officer and office staff with permission from the Director of Operations and/or Finance Officer.

8.6

Marketing and Evaluation Information - Marketing and evaluation information shall be secured in a locked filing cabinet and on a password protected computer, both of which will only be accessed by or with the permission of the Marketing and Communication department.

Article 9 Openness

9.1

Openness - Ophea shall make publicly available information about its policies and practices relating to the management of personal information. This information shall be in a form that is generally understandable.

9.2

Information - The information made available shall include:

- a. the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
- b. the means of gaining access to personal information held by the organization;
- c. a description of the type of personal information held by the organization, including a general account of its use;
- d. a copy of any brochures or other information that explain the organization's policies, standards, or codes.

Article 10 Individual Access

10.1

Individual Access - Upon written request, and assistance from Ophea, 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.

10.2

Amendment - An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10.3

Denial - An individual may be denied access to his or her personal information and provided a written explanation as to why if:

- a. the information is prohibitively costly to provide;
- b. the information contains references to other individuals;
- c. the information cannot be disclosed for legal, security, or commercial proprietary reasons, and
- d. the information is subject to solicitor-client or litigation privilege.

10.4

Contents of Refusal - If Ophea determines that the disclosure of personal information should be refused, Ophea must inform an individual the following:

- a. the reasons for the refusal and the provisions of the Act on which the refusal is based;
- b. the name, position title, business address and business telephone number of the Privacy Officer who can answer the applicant's questions; and
- c. that the individual may ask for a review within thirty (30) days of being notified of the refusal.

10.5

Source - Upon request, the source of personal information shall be disclosed along with an account of third parties to whom the information may have been disclosed.

10.6

Identity - Sufficient information may be required to confirm an individual's identity prior to providing that individual an account of the existence, use, and disclosure of personal information.

10.7

Response - Requested information shall be disclosed within 30 days of receipt of the request at minimal expense for copying or no cost to the individual, unless there are reasonable grounds to extend the time limit. The requested information shall be provided in a form that is generally understandable.

10.8

Costs - Costs may only be levied if an individual is informed in writing in advance of the approximate cost and has agreed to proceed with the request.

10.9

Inaccuracies - If personal information is inaccurate or incomplete, it shall be amended as required and the amended information shall be transmitted to third parties in due course.

10.10

Unresolved Complaints - An unresolved complaint from an individual in regards to the accuracy of personal information shall be recorded and transmitted to third parties having access to the information in question.

Article 11 Challenging Compliance

11.1

Challenges - An individual shall be able to challenge compliance with this Policy and the Act to the designated individual accountable for compliance.

11.2

Procedures - Upon receipt of a complaint Ophea shall:

- a. Record the date the complaint is received and contact information to follow up;
- b. Notify the Privacy Officer who will serve in a neutral, unbiased capacity to resolve the complaint;
- c. Acknowledge receipt of the complaint by way of telephone conversation and clarify the nature of the complaint within three (3) days of receipt of the complaint;
- d. Appoint an investigator using Ophea personnel or an independent investigator, who will have the skills necessary to conduct a fair and impartial investigation and will have unfettered access to all files and personnel, within ten (10) days of receipt of the complaint.
- e. Upon completion of the investigation and within twenty-five (25) days of receipt of the complaint, the investigator shall submit a written report to Ophea.
- f. Notify the complainant the outcome of the investigation and any relevant steps taken to rectify the complaint, including any amendments to policies and procedures within thirty (30) days of receipt of the complaint.

11.3

Assistance - Ophea shall assist an individual in preparing a request for information.

11.4

Whistleblowing - Ophea must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of Ophea, or deny that employee a benefit because the employee, acting in good faith and on the basis of reasonable belief:

- a. has disclosed to the commissioner that Ophea has contravened or is about to contravene the Act;
- b. has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene the Act;
- c. has refused to do or stated an intention of refusing to do anything that is in contravention of the Act.