



## Privacy Policy

---

The Oakville Community Foundation (The Foundation) values its relationships with all of its stakeholders including its donors, fund holders, applicants, volunteers and employees, and is committed to the protection of their personal information. Accordingly, The Foundation adheres to the privacy principles, and accompanying commentary, set out below (the “Privacy Principles”). The Privacy Principles are based on the principles set out in Schedule I of the Personal Information Protection and Electronic Documents Act (Canada) (the “Act”). “Personal Information”, as used in this Policy, means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

We acknowledge that the Act may not apply to The Foundation however, it is our intention to be guided by it and to practice in accordance with its principles.

It is also our intent to include all organizations who may be donors, fund holders or applicants in our privacy practices. We will use the term “individual” in this Policy, however, it will include those organizations unless the context clearly implies otherwise.

### **Principle 1 – Accountability**

#### **The Foundation is responsible for all Personal Information under its control.**

Accountability for our compliance with the Privacy Principles rests with our Chief Executive Officer, even though other individuals within The Foundation have responsibility for the day-to-day collection and processing of Personal Information and may be delegated to act on behalf of the Chief Executive Officer.

We are responsible for Personal Information in our possession or control, including information that has been transferred to a third party for processing. We restrict the transfer of such Personal Information to third parties as much as is reasonably possible, and we use contractual or other means to provide a comparable level of protection when the information is transferred to a third party.

### **Principle 2 – Identifying Purposes**

#### **We will identify and document the purposes for which we collect, use, or disclose Personal Information at or before the time of collection.**

The purposes will be limited to those which are related to our mission and which a reasonable person would consider are appropriate in the circumstances.

We collect, use, and disclose Personal Information concerning our donors and fund holders for the following reasons:

- To acknowledge their support.
- To solicit their on-going support.
- To advise them of the activities of The Foundation and about developments in the community which may be of interest.
- To publicize our grants and awards and their contributions to The Foundation.
- To understand their goals and objectives.

It is the policy of The Foundation that our donors and fund holders may at any time “opt-out” of any disclosure of their Personal Information except as required by law.



We collect, use, and disclose Personal Information concerning our applicants for the following reasons:

- To review and consider their applications for grants and awards.
- To understand their goals and objectives.
- To publicize our grants and awards.

We collect, use, and disclose Personal Information concerning our employees for the following reasons:

- To manage our organization effectively.
- To establish and manage benefit programs.

We collect, use, and disclose Personal Information concerning our volunteers for the following reasons:

- To solicit their on-going support.
- To advise them of the activities of The Foundation and about developments in the community which may be of interest.

We collect, use, and disclose Personal Information from all of our stakeholders in order to meet our legal, statutory or regulatory requirements.

If we plan to use or disclose Personal Information we have collected for a purpose not previously identified, we will identify and document this purpose, orally or in writing, to the individual from whom the Personal Information has been collected, before such use or disclosure.

We will make a reasonable effort to specify the identified purposes, orally or in writing, to the individual from whom the Personal Information is collected either at the time of collection or after collection but before use. We will state the identified purposes in such a manner that an individual can reasonably understand how the information will be used or disclosed.

### **Principle 3 – Consent**

#### **Personal Information will only be collected, used, or disclosed with the knowledge and consent of the individual, except where inappropriate.**

The way in which we seek consent, including whether it is express or implied, may vary depending upon the sensitivity of the information and the reasonable expectations of the individual. An individual can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. We will inform individuals of any implications of withdrawing consent.

Typically, we will seek consent for the use or disclosure of information at the time of collection. In certain circumstances, consent may be sought after the information has been collected but before use (such as where we want to use information for a purpose not previously identified).

We will not, as a condition of the supply of services, require an individual to consent to the collection, use, or disclosure of Personal Information beyond that required to fulfil the explicitly specified and legitimate purposes.

In certain circumstances, as permitted or required by law, we may collect, use or disclose Personal Information, without the knowledge or consent of the individual. These circumstances include: Personal Information is publicly available as defined by regulation; where collection or use is clearly in the interests of the individual and consent cannot be obtained in a timely way; to investigate a breach of an agreement or a contravention of a law; to act in



respect to an emergency that threatens the life, health or security of an individual; for debt collection; or to comply with a subpoena, warrant or court order.

We confirm that it is our policy to allow our donors and fund holders to opt-out, either initially or at any time thereafter, of any disclosure of their Personal Information.

#### **Principle 4 – Limiting Collection**

**We will limit the amount and type of Personal Information collected to that which is necessary for our identified purposes and we will only collect Personal Information by fair and lawful means.**

##### **a) Links to/from External Sites:**

The Foundation uses technologies, such as cookies, to customize content and advertising, and that provide social media features that enable better analysis of traffic to our website.

#### **Principle 5 – Limiting Use, Disclosure, and Retention**

**Personal Information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual, as required by law, or as otherwise outlined or provided in these Policy Principles. Personal Information will be retained only as long as necessary to fulfil the identified purposes.**

Personal Information which has been used to make a decision about an individual will be retained long enough to allow the individual access to the information after the decision has been made and, in the event of an access request or a challenge, long enough to exhaust any recourse an individual may have under the law. Where Personal Information is no longer required to fulfil the identified purposes, it will be destroyed, erased, or made anonymous.

#### **Principle 6— Accuracy**

**We will use our best efforts to ensure that Personal Information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.**

We will use our best efforts to ensure that Personal Information that is used on an on-going basis, including information that is disclosed to third parties, and information that is used to make a decision about an individual, is accurate, complete, and up-to-date.

#### **Principle 7— Safeguards**

**We will protect Personal Information with safeguards appropriate to the sensitivity of the information.**

Our safeguards will protect Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, regardless of the format in which the information is held. Our employees are trained to ensure that they are aware of the importance of maintaining the confidentiality of Personal Information, and we exercise care in the disposal or destruction of Personal Information to prevent unauthorized parties from gaining access to the information.



Our methods of protection include physical measures (for example, locked filing cabinets and restricted access to offices), organizational measures (for example, security clearances and limiting access on a “need-to-know” basis), and technological measures (for example, the use of passwords and encryption).

### **Principle 8— Openness**

**We will make specific information about our policies readily available, except to the extent this is confidential commercial information.**

The information we will make available will include: how to gain access to Personal Information; the type of Personal Information held by us, including a general account of its use; general information concerning our Policy and policies; what Personal Information is made available to related companies; and how to contact our Chief Executive Officer.

### **Principle 9— Individual Access**

**Upon written request, we will inform an individual of the existence, use, and disclosure of his or her Personal Information and we will give the individual access to that Personal Information. An individual can challenge the accuracy and completeness of his or her Personal Information and have it amended as appropriate.**

We will respond to an individual’s written request within a reasonable time (generally within 30 days). We will need to confirm the individual’s identity before providing access. We will assist any individual who informs us that they need assistance in preparing a request. We may require an individual to provide sufficient information to permit us to provide an account of the existence, use, and disclosure of Personal Information. While our response will typically be provided at no cost to the individual, depending on the nature of the request and the amount of information involved, we reserve the right to impose a cost. In these circumstances, we will inform the individual of the approximate cost to provide the response and proceed upon payment by the individual of the cost. Requested information will be provided or made available in a form that is generally understandable. Where possible, we will indicate the source of the information.

In providing an account of third parties to which we may have disclosed Personal Information about an individual, we will attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which we have actually disclosed Personal Information, we will provide a list of organizations to which we may have disclosed the information.

If an individual successfully demonstrates the inaccuracy or incompleteness of Personal Information, we will amend the information as required. If a challenge is not resolved to the satisfaction of the individual, we will record the substance of the unresolved challenge. Where appropriate the amended information or the existence of the unresolved challenge, as the case may be, will be transmitted to third parties having access to the information in question.

In certain situations, we may refuse a request or not be able to provide access to all the Personal Information we hold about an individual. Exceptions to the access requirement will be limited and specific, as permitted or required by law. Where permitted, the reasons for denying access will be provided to the individual upon request. Exceptions may include: information that contains references to other individuals or contains confidential commercial information, where such information cannot be severed from the record; information collected in the course of investigating a breach of an agreement or in the course of a formal dispute resolution process; and information that is subject to solicitor-client privilege.

## **Principle 10 – Challenging Compliance**

### **Any individual can address a challenge concerning our compliance with any of the Privacy Principles to our Chief Executive Officer.**

We will investigate all written complaints. If we find a complaint to be justified, we will take all appropriate measures, including, if necessary, amending our policies and practices.

Any questions or complaints about our Privacy Policy can be directed to our Privacy Officer. Our address for communication is 410 North Service Road East, Suite 200, Oakville, ON L6H 5R2. We may also be reached by fax, 905-845-1395. Our Chief Executive Officer may be reached by e-mail at [wendy@theocef.org](mailto:wendy@theocef.org).

If we do not resolve the issue to your satisfaction, you may contact:

The Privacy Commissioner of Canada  
112 Kent Street  
Ottawa, ON K1A 1H3

## **Principle 11 – Amendments**

**We will from time to time review and revise our privacy practice and this Privacy Policy. In the event of an amendment, a notice will be posted on our website: [www.theocf.org](http://www.theocf.org), or in our office, or in other appropriate Oakville Community Foundation communications. Any changes will apply from the date of posting on our website.**

## **Principle 12 – Process and Procedures**

Where a security breach of Personal Information has occurred, the following procedures are in place:

- The Foundation shall disclose to the individual any breach of security safeguards involving the individual's Personal Information under its control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual;
- The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from the breach or to mitigate that harm;
- The notification shall be given as soon as possible after the Foundation determines that the breach has occurred;
- For the purposes of this principle, 'significant harm' includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property; and, The Foundation will assess whether there is a real risk of significant harm to the individual with respect to, without limitation, (a) the sensitivity of the Personal Information involved in the breach, (b) the probability that the Personal Information has been, is being, or will be misused; and, (c) any other factor the Foundation may consider relevant.



**POLICY AMENDMENT AND REVIEW**

The Board of Directors may amend these policies at any time.

**REVISION HISTORY**

Approved: April 2006

Amendment Approved by Board of Directors December 7, 2016

Amendment Approved by Boar of Directors April 11, 2018

Approved by Board of Directors December 11, 2019