

EWB Best Practices Privacy Policy

Engineers Without Borders Canada (EWB-Canada) is committed to protecting the privacy of its donors, volunteers, employees, members and other stakeholders.

To support this commitment, EWB-Canada has adopted the Canadian Centre of Philanthropy's Code of Fundraising Ethics and the Bill of Donor's Rights. EWB-Canada is dedicated to being both transparent and accountable in dealing with the information that you choose to share with us.

During the course of our various projects and activities, EWB-Canada frequently gathers and uses personal information. Anyone from whom we collect such information should expect that it will be carefully protected and that any use of or other dealing with this information is subject to consent. EWB-Canada's privacy practices are designed to achieve this.

Personal Information Defined

Personal Information is any information that can be used to distinguish, identify or contact a specific individual. This information can include an individual's opinions or beliefs, as well as facts about, or related to, the individual. Exceptions: business contact information and certain publicly available information, such as names, addresses and telephone numbers as published in telephone directories, are not considered personal information.

Privacy Practices

Personal information gathered by EWB-Canada is kept in confidence. Our personnel are authorized to access personal information based only on their need to deal with the information for reason(s) for which it was obtained. Safeguards are in place to ensure that the information is not disclosed or shared more widely than is necessary to achieve the purpose for which it was gathered. We also take measures to ensure the integrity of this information is maintained and to prevent its being lost or destroyed.

We collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in light of the circumstances. We routinely offer individuals we deal with the opportunity to opt not to have their information shared for purposes beyond those for which it was explicitly collected.

Website and Electronic Security

EWB-Canada uses password protocols to protect personal and other information we receive. Our software is routinely updated to maximize protection of such information. We use your IP address to help diagnose problems with our server, and to administer our website.

Linking to Other Sites

This site contains links to other sites. EWB-Canada is not responsible for the privacy practices or the content of such Web sites.

Contact Information

Questions, concerns or complaints relating to EWB-Canada's privacy policy or the treatment of personal information should be emailed to: privacy@ewb.ca.

Further information on privacy and your rights in regard to your personal information may be found on the website of the Privacy Commissioner of Canada (www.privcom.gc.ca).

Principles

- 1) **Accountability:** Organizations are responsible for all personal information under their control and remain responsible when personal information is processed by third parties on their behalf.
 - Appoint an individual (staff or volunteer) to be a “Chief Privacy Officer.” This person might not be a fundraiser, and the CPO role only part of their overall responsibilities.
 - They don’t need to have this title, just the responsibilities that it suggests. All staff must know who this person is. The CPO has responsibility for understanding the broad impact of privacy, for the implementation of policies and procedures, and is responsible for handling complaints. See Appendix F.
 - Ensure third party contracts contain a provision explicitly requiring adherence to privacy legislation.

- 2) **Identifying purpose:** Organizations are required to document purposes before they can collect and use personal information.
 - The purpose for which personal information is collected must be clear and obvious.
 - Use purpose statements (Appendix B) where multiple purposes are planned.
 - Don’t forget that information already in your possession can only be used for the original purpose for which it was collected. If you want to add a purpose (i.e. new newsletter to all donors) you must inform individuals of the change.
 - Many fundraising related activities may not fall under the definition of commercial activity and therefore consent would not be required prior to collecting information.

- 3) **Consent:** Knowledge and consent of the individual are required to collect, use or disclose personal information.
 - Consent must be meaningful. That is it must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.
 - See sample purpose statements (Appendix B). Post statements related to the purpose of collecting, using and disclosing personal information wherever you can: on your website, in newsletters, on posters and brochures, etc.
 - Appropriate consent varies with the sensitivity of the personal information. See definitions of implied and express consent.

- Consent may be given in many ways. Consent may be given orally. A signed form that contains a clear purpose statement is a means of providing express consent. A check-off box on a direct mail coupon may be used to allow individuals to request that their names and addresses are not given to other organizations. Individuals who do not check off the box may be assumed to have consented to the transfer of this information to third parties.
- An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. You must have a means to allow individuals to easily opt out and the procedures in place to record and respect this request.

4) Limiting collection: The amount and type of information is limited to what is necessary for identified purpose.

- Information collected must be limited to that which is necessary to fulfill the purposes identified. Why do you collect birthdays on donor reply coupons?
- New purposes require new consent.

5) Limiting use, disclosure and retention of personal information:

Information can only be disclosed or used for the purposes for which it was collected.

- Personal information that is no longer required should be destroyed, erased or made anonymous. You should have guidelines for the destruction of personal information.

6) Accuracy: Personal information has to be accurate, complete and as up to date as is necessary for the purposes for which it is to be used.

- 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 individual.
- An organization must not routinely update personal information unless such a process is necessary to fulfill the purposes for which the information was collected.

7) Safeguards: Organizations must take steps to protect personal information from theft and loss, as well as unauthorized access, disclosure, copying or use.

- Physical measures (locked filing cabinets, restricted access to offices, etc.), organizational measures (security clearances, “need-to-know” access, etc.) and technological measures (passwords, encryption, etc.) must all be used.

- Staff and volunteer training are also key elements in a sound privacy policy. Have all staff and volunteers sign an annual statement related to maintaining the confidentiality of personal information.

8) Openness: Organizations must provide the public with general information on their personal information protection policies and practices and must make it easy to identify and contact the person responsible for personal information protection.

- Give individuals easy access to your privacy policies and practices. Use newsletters, posters, brochures, websites, etc. to post information.
- Make the information clear and understandable – think about your audience.
- Again, train staff – particularly reception staff.
- Be sure to provide the name and contact information of the individual you have identified as your “Chief Privacy Officer.”

9) Individual access: Upon request, individuals must be informed of the existence, use and disclosure of all their personal information and be given access to that information. An individual has the right to challenge the accuracy and completeness of the information and have it amended as appropriate.

- Individuals have the right to be given access their personal information (exceptions should be limited and specific and may include information that contains references to other individuals, or information that cannot be disclosed for legal, security or other reasons.) Individuals may correct inaccuracies in their own personal information.
- Requests for access must be responded to within a reasonable time – no more than 30 days and at minimal or no cost to the individual.
- Think about the information in your files. If someone asked to access their file, what would they find and how would you feel about that individual seeing this information?

10) Challenging compliance: An individual can challenge an organization’s compliance to the code, and an organization must develop procedures to handle complaints.

- Again, you need a complaints policy. The legislation is a complaint driven process.
- You must be able to demonstrate that you have policies and procedures in place that are being followed.
- Your “Chief Privacy Officer” should receive and respond to all privacy complaints.
- You must be prepared to amend policies and procedures if the complaint has validity.
- In general, if an organization is operating under these 10 principles, it will tend to be in compliance with PIPEDA.