Privacy Policy Checklist

Why do registered charitites need to have a privacy policy?

Legislation has been enacted by the federal government (*Personal Information Protection and Electronic Documents Act* (PIPEDA)) and some provinces (including BC, Alberta, and Quebec) dealing with the use of personal information. Depending on the type of information and the use(s) made by the charity of the information, one or more of these statutes may apply.

Many charities are confused about whether to comply with federal or provincial privacy law. The general rule is set out in the "privacy compliance principle":

> ***If a province's privacy law has been ruled to be "substantially similar" (such as in Alberta, British Columbia, and Quebec) to the federal law by the Privacy Commissioner of Canada, then the provincial law supersedes the federal law. This means that the registered charity has to comply with provincial legislation only.***

However,

- If the provincial law is not considered to be "substantially similar" to PIPEDA, then registered charities operating in that province must comply with both the federal and provincial laws.
- If a province does not have specific privacy legislation, then registered charities must comply with PIPEDA.
- Registered charities working across provincial borders have to comply with the different laws of each province in which they operate (as well as abiding by any federal restrictions applicable to their inter-jurisdictional transactions).
- Charities in subsectors such as health may be subject to narrow privacy legislation dealing specifically with particular aspects of the field in which they operate (e.g., collection and use of patient information) and that may be enacted to complement or supplement broad-based federal or provincial privacy legislation

PIPEDA in brief

- Organizations may fall under the Act based on their activities and/or based on their dealings with their employees. Activities do not trigger the Act unless they are commercial transactions.
- Organizations covered by the Act must obtain an individual's consent when they collect, use, or disclose an individual's personal information.
- Consent may be expressed or implied, and the type of consent necessary will depend on the type of information being collected.
- Charities should obtain positive consent, for example, "I give permission for my information to be shared…"—when the information is more sensitive (e.g., disclosing donor financial data).
- Charities may obtain negative consent, for example, "Check this box if you do not want your information to be shared…" when the information is less sensitive (e.g., using past sales data to contact stakeholders about an updated version of a product previously purchased from the charity).
- Charities may rely on implied consent when the information is not sensitive and is closely associated with the expected use (e.g., accessing member information to provide membership benefits).
- Consent is not necessary when the information is publicly available (e.g., information that can be found in the telephone book) or if it is used solely for journalistic, artistic, or literary purposes.
- An 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 be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords, and encryption.

The following checklist provides general guidance for organizations interested in assessing their information-handling practices. It may also be used as a guide to draft your own privacy policy, ensuring that you address any unique areas of concern in information-handling practices for your organization. This checklist does not go into detail regarding specific statutory or regulatory compliance requirements; rather, it identifies key sections and points to consider when creating or reviewing your organization's privacy policy.

We suggest you seek legal advice to verify that the final policy complies with your organization's legal and regulatory obligations.

Checklist

Ideal components of a privacy policy	Questions to ask yourself	Included	Needed
Introduction			
Clearly state the intent or purpose of the policy.	Is it intended for members, clients, customers, and/or employees? Be specific.	☐	☐
Consider the language and style of the policy. Try as much as possible to use plain language.	Does the language suit your clientele or users?	☐	☐
Include a brief overview of the organization.		☐	☐
Indicate if the policy is a public document.		☐	☐
If applicable, refer to other relevant policies or procedures within your organization.		☐	☐
Explain that personal information will be handled by your organization in accordance with the privacy policy and PIPEDA and/or provincial legislation and any applicable laws, regulations, codes, and so on.	If you operate solely within one province, does your provincial legislation supersede the federal legislation?	☐	☐
Data Collection			
Describe what types of data your organization collects and why.	Do you maintain membership, donor, or purchase lists?	☐	☐
Describe what is meant by personal information.		☐	☐

Ideal components of a privacy policy	Questions to ask yourself	Included	Needed
Describe how consent from individuals will be obtained. NOTE: There are two types of consent: expressed and implied. Consent may be **expressed** verbally or in writing.	Are you seeking consent in writing? Do you have a written form for the individual to sign? Does it require them to positively agree to the use of their information or ask them to indicate if they do not want their information shared? If you use a written form, where will you keep the signed consent?	☐	☐
When consent is **implied**, the charity assumes that the person to whom the personal information pertains to have agreed to its collection and use for a specific purpose without having requested or received any explicit affirmation that the person agrees or indication that the person does not consent. An example of implied consent is the collection and use of member information to provide benefits to members.	Are you implying consent? Have you indicated your intentions for use or sharing of the information without asking for consent? Is the use of the information implicit in your reason for collecting it? For example, do you use the information to provide member benefits?	☐	☐
Describe what methods your organization uses to collect personal information.	Do you collect and/or keep information on forms in hard copy, on computers, and/or on your website? What security is necessary to protect the information given the location and format in which it is kept?	☐	☐
Indicate that the information is necessary for the activities of the organization	Can you assure stakeholders that the data is collected only for the purposes stated?	☐	☐

Ideal components of a privacy policy	Questions to ask yourself	Included	Needed
Use of Data			
Generally describe how the organization will use the personal information collected.	Will the data be used for more than personal contact with your stakeholders? Given the proposed use, is consent implied when the information is collected or is express consent more appropriate. If express consent is needed, how do you propose to obtain consent?	☐	☐
Disclosure			
Describe under what circumstances the information might be disclosed, if any.	Will the lists be used by third parties? If so, how do you propose to obtain consent and what additional measures will you need to have in place to protect the security of the information (e.g., provisions in the contract with the third party) when it is used by the third party?	☐	☐
Provide examples or instances where the information will be used.	Do third party services, such as fundraisers or marketing agents, need access to the information in order to perform their duties? Could sharing the information provide the opportunity for third parties to promote products or services to the stakeholder whose information you are providing? What consent and security measures are necessary if this is the case?	☐	☐

Ideal components of a privacy policy	Questions to ask yourself	Included	Needed
Use of Data in Marketing or Fundraising			
Include an explanation of how data will be used if the organization implements a direct marketing campaign or other type of fundraising effort.	How many hands will the information pass through? (Remember print shops and volunteers who stuff envelopes.)	☐	☐
Have options for individuals to opt in to or out of marketing campaigns.		☐	☐
If applicable, explain how the organization deals with information in third party contracts and if names are shared.	Can you assure stakeholders that third parties will maintain comparable levels of protection? (e.g., does your contract with the third party provide for this)?	☐	☐
Accuracy (Integrity of the data)			
Describe steps taken to ensure information is accurate, complete, and up-to-date.	How often will you check with your stakeholders to be sure the information is accurate?	☐	☐
Describe how an individual can correct personal information.		☐	☐
Security			
Show that reasonable steps have been taken by the organization to safeguard personal information in the event of misuse, loss, unauthorized access, or disclosure.	What security measures are in place for print and digital records? Where material that includes personal information is collected offsite or where records that include personal information leave the charity's premises for a legitimate reason, what systems or measures are in place to safeguard it?	☐	☐

Ideal components of a privacy policy	Questions to ask yourself	Included	Needed
Disposal of records			
Explain what reasonable steps will be taken to permanently dispose of the records when no longer required.	How will you dispose of print and digital copies of records? Are archived records that must be kept to comply with legal requirements (such as those under the *Income Tax Act*) seperated from current databases?	☐	☐
Access to the information			
Explain an individual's right to his or her own personal information.		☐	☐
Indicate who has access to the information.	Is the information accessible to staff, board members, and volunteers? Does anyone else have access? Do only those people with a legitimate need for the information have access to it?	☐	☐
Describe when access might not be granted, if any.		☐	☐
Explain when fees will be charged for providing the information to the person it pertains to, if any.	Will you charge a fee for processing the information request or the related photocopying costs?	☐	☐
Organizational contact			
Identify how and who to contact in the organization regarding the policy.	In addition to who and how, what is your timeliness of replies to inquiries?	☐	☐
Explain how complaints can be made and to whom.		☐	☐
Date, version and name of the person who drafted the policy		☐	☐

General Information Resources

Office of the Privacy Commissioner of Canada (OPCC) - **www.priv.gc.ca/index_e.cfm**

Fact Sheets - The Application of the *Personal Information Protection and Electronic Documents Act* to Charitable and Non-Profit Organizations - **www.priv.gc.ca/fs-fi/02_05_d_19_e.cfm**

OPCC – Information for Organizations - **www.priv.gc.ca/resource/io_e.cfm** and **www.priv.gc.ca/information/guide_e.pdf**

Links to Provincial/Territorial Privacy information and legislation - **www.priv.gc.ca/resource/prov/index_e.cfm**

FAQs for Alberta Not-for-Profit Organizations - **http://pipa.alberta.ca/index.cfm?page=faqs/NonProfitFAQs.html**

E: info@charitycentral.ca

Government of Canada Gouvernement du Canada
Canada
Production of this fact sheet has been made possible by a financial contribution from the Canada Revenue Agency.