

# Aptlaw.com

A law newsletter for charities and NFPs by Adam Aptowitzer LL.B.

Adam Aptowitzer, LL.B.  
adam@aptlaw.com  
Phone 416.712.2218  
Fax 416.850.6087  
<http://www.aptlaw.com>

Contact [Adam Aptowitzer](#)

[Click here to see how we can help](#)

## Practical PIPEDA for Charities and NPOs - Part II

This is the third of a four part series on the Personal Information Privacy and Electronic Documents Act (*PIPEDA*). By way of review, *PIPEDA* is based on the Canadian Standards Association's Model Code for the Protection of Personal Information. The code has ten principles, which, loosely categorized, govern the collection, use, and handling of personal information. A list of these principles and commentary on each of them is available at the website of the [Privacy Commissioner of Canada](#).

The first part of this series dealt with the application of PIPEDA to charities and not-for-profits ([click here to see a copy](#)). The second part dealt with the privacy implications of collecting information (you can view a copy by [clicking here](#)). This newsletter deals with the storage and use of personal information. Five out of the ten PIPEDA principles deal with these topics, they are:

- 1) [Limited Use, Disclosure and Retention](#)
- 2) [Accuracy](#)
- 3) [Safeguards](#)
- 4) [Openness](#)
- 5) [Individual Access](#)

### 1. Limited Use, Disclosure and Retention

Broadly, this principle requires the organization to use the information collected only for the purposes for which the individual has consented or which the law requires. For example, if an individual attending a fundraiser has given their personal information to the organization in order to purchase a seat at the fundraiser, his or her name cannot be added to a general mailing list unless they have given their specific consent. Furthermore, information, which has served the purpose for which it was collected, must be destroyed unless a new consent was obtained for the use of this information in a new context. (You should also have guidelines governing the destruction of personal information).

### 2. Accuracy

Collected personal information must be accurate, complete and up-dated as necessary for the purposes for which it is to be used. This obligates the organization to put in place measures for continuous updating of the information they control. However, the organization cannot do this unless the updating of information is necessary to complete the purpose for which the information was collected in the first place. This underscores the need for intelligent drafting of the request for consent in the first place. If the consent were for any reason to become 'stale' the organization may not update the information but rather would be obligated to destroy it.

### 3. Safeguards

PIPEDA requires that collected information be protected by appropriate measures from unauthorized access, disclosure, copying, use or modification. The safeguards taken by any particular organization will necessarily be specific to its circumstances. Personal information should be protected by: physical safeguards (i.e. locked filing cabinets, offices and other rooms), technological safeguards (i.e. passwords, encryptions and firewalls), and organizational measures (i.e. security clearances and limited access to information). Organizations should audit and update their security measures regularly. [Contact me](#) for help conducting your security audit.

### 4. Openness

The organization should make its information handling policies and practices readily available to the public. In particular, you should make available on your website or through a brochure the name and contact information for the person in your organization who is accountable for privacy policies and practices, and how an individual can access his or her personal information held by the organization. The policy of openness should be well thought out as it is the most public way your organization's approach to privacy issues will be evaluated and could become a significant addition to your public relations program if done comprehensively and correctly or a liability if handled improperly.

### 5. Individual Access

Upon request, an individual must be informed of the existence and use of his or her personal information and its disclosure, and be given access to their personal information. An individual has the right to challenge the accuracy of that information and have it amended if necessary. The barriers to an individual to view their information should be minimal (i.e. requests for access should be responded to quickly and without cost). Also, the organization must be careful not to release the information of other individuals which might be connected to the information request.

For more information on these or any other legal issues affecting your charity or not-for-profit organization, [contact me](#).

Charitably,

Adam

[clicking here](#)

Adam Aptowitz distributes the above newsletter on the understanding that it does not constitute legal advice or establish the solicitor/client relationship by way of any information contained herein. The contents are intended for general information purposes only and under no circumstances can it be relied upon for legal decision-making. This newsletter is current only as of the date above and does not reflect any subsequent changes in the law. Readers are advised to consult with a qualified lawyer and obtain a written opinion concerning the specifics of their particular situation.