Guidelines for Developing a Privacy Policy Under the *Personal Information Protection Act* (PIPA)

May 20, 2004
(Replaces version of: new document)

May 20, 2004

Purpose Of This Document

This document is a guide for organizations[1] to refer to when developing a privacy policy under the Personal Information Protection Act ("PIPA").

PIPA applies to more than 350,000 private sector organizations in British Columbia, including businesses, charities, associations and labour organizations. It sets out rules about how those organizations may collect, use and disclose personal information.

PIPA requires each organization to establish a set of policies and procedures for complying with PIPA. It also requires organizations to make their policies and procedures available to the public.

Privacy policies may take many forms, depending on the size of the organization, the quantity and type of personal information it collects, uses or discloses, and the nature of those activities. This guide is organized to highlight the elements required in a privacy policy. Your organization may also choose to use headings of a similar nature in order to assist individuals in understanding your privacy policy.

Part 1: Introduction

Your policy should explain to those individuals whose personal information you collect, use or disclose—including your employees—why you developed your policy. For example:

- Express your commitment to being accountable for how you treat personal information and for the principles outlined in your policy.
- Say that the policy is developed in compliance with British Columbia's *Personal Information Protection Act* ("PIPA").
- Briefly explain what PIPA is—for example, "B.C.'s *Personal Information Protection Act* sets out rules for how organizations such as ours can collect, use and disclose your personal information".

Part 2: What is Personal Information?

It would be helpful to explain the definition of "personal information" in your policy—for example, "Personal information means information about an identifiable individual, such

[1] An "organization" includes a person (except where acting in personal or domestic capacity or acting as an employee), an unincorporated association, a trade union, a trust or a not-for-profit organization. See the definition under section 1 of PIPA for information regarding exclusions.

as someone's name, home address, social insurance number, sex, income or family status."

Your policy should also explain the definition of "employee personal information" if you have employees to whom the policy applies. The following are examples of definitions that should be included in your policy:

- **Employee personal information** is information that is collected, used or disclosed solely for the purposes reasonably required to establish, maintain, manage or terminate an employment relationship between an employee (including a volunteer) and an organization. This may include information such as name, home address, educational history and employment history. This does not include *contact information* or *work product information* (see below).

- **Contact information** means information that allows an individual to be contacted at work. It includes the name, position name or title, business telephone number, business address, business e-mail and business fax number for the individual.

- **Work product information** is information that is prepared or collected by an employee as part of that individual's work responsibilities, but does not include information about an individual who did not prepare or collect the information.

Part 3: Organizations to which the policy applies

If your privacy policy extends to other organizations, such as corporate affiliates or subsidiaries, say so and, if feasible, provide a list of those organizations. Be careful to ensure that you are completely familiar with the personal information that those organizations collect, use or disclose, and that your policy truly does apply to those organizations.

Part 4: Why you collect and use personal information

Explain what personal information your organization collects and describe the purposes for which it uses that personal information:

- List all of the purposes for which you collect, use or disclose personal information. Examples might include: to verify identity, to verify credit-worthiness, to provide requested services or products, or to enrol an individual in a program.

- Give a general description of the personal information you collect and use. Examples might include: name, birth date, home mailing address, home phone number, income, age and product preferences.

- It may be helpful to list the kinds of personal information in relation to each purpose for collection, so it is clear to individuals how the collection of their personal information and its uses are related.

Part 5: Limits on collection, use, and disclosure

The policy should set out the limits on its collection, use and disclosure of personal information by stating the following:

- Your organization will only collect and use personal information that is necessary to fulfill the purposes you identify in the policy.

- Your organization will not collect, use or disclose personal information except for the identified purposes unless your organization has received further consent from the individual.

- Your organization will only collect, use or disclose personal information in accordance with PIPA.

Part 6: How you disclose personal information

Explain under what circumstances your organization discloses personal information to other organizations or to government bodies:

- Describe the circumstances under which the purposes for collection and use of personal information, identified above, require you to disclose personal information outside your organization.

- If your organization retains another organization to do work for you that involves personal information, say that your organization will ensure there is an agreement in place that commits the organization providing services to adhere to your organization's privacy policy.

- You may wish to state that your organization will disclose personal information where authorized by PIPA or required by law—examples of a legal requirement to disclose include a court order, subpoena or search warrant.

- Assure individuals that your organization will not sell or rent personal information to anyone outside your organization unless those individuals have given consent in accordance with PIPA.

Part 7: How you obtain consent to collect, use, and disclose personal information

Explain how your organization gets consent to collect, use or disclose personal information. Here are some suggestions:

- Your organization may wish to explain that your organization will get individuals' consent to collect, use or disclose their personal information, except where you are legally authorized or required by law to do so without consent.

- If there are any situations where your organization may collect, use or disclose personal information without an individual's knowledge or consent—as allowed under PIPA sections 12, 15 and 18—you should say so and list them specifically.

- Your policy should explain that individuals can consent orally, in writing or electronically and that their consent may be implied or express depending on the nature and sensitivity of the personal information.

- It may help to explain that individuals are considered to have given implied consent when your purpose for collecting, using or disclosing personal information would be considered obvious and the individual voluntarily provides personal information for that obvious purpose.

- Your should explain that you will tell individuals your purpose for collecting personal information and give them a chance to refuse to give you their personal information or a chance to withdraw their consent later.

- Explain that individuals may withdraw their consent at any time by giving your organization reasonable notice, but tell individuals they cannot withdraw consent where doing so would frustrate performance of a legal obligation (such as a contract between the individual and your organization).

- Explain that, when individuals tell you they are withdrawing consent, PIPA requires you to tell them of the likely consequences of withdrawing consent (such as your being unable to provide them with services or goods that require their personal information).

- In the case of *employee personal information*, explain that PIPA allows your organization to collect, use or disclose employee personal information without consent if it is reasonable for the purposes of establishing, managing or terminating an employment relationship between your organization and the individual. (Note that, in such cases, PIPA still requires your organization to notify employees of the collection, use or disclosure.)

Part 8: How long you retain personal information

Your policy should explain how long your organization keeps personal information:

- You should explain that your organization will keep personal information used to make a decision that directly affects individuals for at least one year after you make that decision. (PIPA requires this.)

- Your policy should explain that, subject to the above one-year retention requirement, your organization will only retain personal information for as long as necessary to fulfil the identified purposes or as long as required for a legal or business purpose. Be as specific as you can about how long information is retained.

Part 9: How You Keep Personal Information Secure

You should provide assurances that personal information under your organization's custody or control is kept secure:

- You should say that your organization has security arrangements to prevent against risks such as unauthorized access, collection, use, disclosure, copying, modification or disposal of personal information.

- You should list, if you can, the main methods you use to keep personal information secure.

- Your policy should explain that you will use reasonably secure methods whenever you destroy personal information.

Part 10: How you ensure that personal information is accurate

Your policy should address your organization's commitment to ensuring that the personal information is accurate. Here are some suggestions:

- Explain that your organization will make reasonable efforts to ensure that the personal information you collect, use or disclose is accurate and complete.

- Explain that individuals may write to you to ask you to correct any errors or omissions in their personal information that is under your organization's control.

- Say that, if your organization is satisfied that an individual's request for correction is reasonable, you will correct the personal information as soon as reasonably possible.

- Explain that your organization will, as soon as reasonably possible, also send an individual's corrected personal information to each organization it was disclosed to during the year before your organization corrected it.

- Explain that, if your organization does not correct an individual's personal information, you will note the requested correction on copies of the personal information under your custody or control.

Part 11: How you provide individuals with access to their personal information under your control or custody

Your policy should explain that individuals can gain access to their personal information under your organization's custody or control. Your policy should, at a minimum, say the following:

- Individuals have the right to access their personal information under your organization's custody or control.

- A request for access must be made in writing.

- Your organization may require individuals to prove their identity before giving them access to their personal information.

- Your organization will give individuals their personal information under your control, information about the ways in which their information is or has been used, and the names of the individuals and organizations to which their personal information has been disclosed.

- PIPA allows your organization to charge a "minimal" fee for providing an individual with access to his or her personal information.

- If a fee is required, your organization will give the individual a written fee estimate in advance.

- Your organization may require payment of a deposit or the whole fee before releasing the requested information.

- Your organization will provide requested personal information within 30 business days after it is requested or you will give written notice if you need more time to respond.

- In some cases, your organization may not give an individual access to certain personal information where authorized or required by PIPA to refuse access.

- If your organization refuses an access request, you will tell the applicant in writing, stating the reasons for your refusal and outlining further steps that are available to the applicant (including any internal review by your organization and the right to ask the Office of the Information and Privacy Commissioner for British Columbia to review the decision).

Part 12: How individuals can complain, ask for access or ask questions

Individuals need to know how they can complain about your organization's treatment of their personal information, how to ask for access to their own personal information or simply how to ask questions:

- Your policy should give the contact information for the person in your organization who is responsible for your compliance with PIPA.

- Your should state that, if individuals are not satisfied with your organization's response, they can complain to the Office of the Information and Privacy Commissioner for British Columbia.

IMPORTANT NOTE

The suggestions contained in this document are for information only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia ("OIPC") with respect to any matter within the jurisdiction of the Information and Privacy Commissioner under PIPA. The guidelines do not affect the powers, duties or functions of the Information and Privacy Commissioner regarding any complaint, investigation or other matter under or connected with PIPA, respecting which the OIPC will keep an open mind. Responsibility for compliance with PIPA remains with each organization.