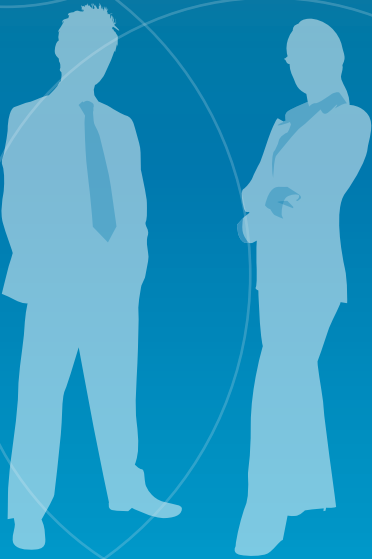




Office of the
Privacy Commissioner
of Canada

PIPEDA

Privacy Guide for Small Businesses: **The Basics**



Privacy is the best policy

Handling privacy concerns correctly can help improve your organization's reputation.

When you take privacy rights seriously in your business, you establish an atmosphere of trust that keeps customers loyal and attracts the best employees. When you establish a comprehensive privacy policy that customers and employees can understand, you are also less likely to become involved in a privacy dispute.

This booklet is an easy-to-use guide prepared by the Office of the Privacy Commissioner of Canada as a first step for businesses that wish to improve their privacy practices and avoid investigations. The tips here will help you build capacity in-house to handle issues and complaints as they arise.

The Office of the Privacy Commissioner of Canada

At the Commissioner's Office, we understand that businesses—especially those that are small and medium-sized—are challenged on a daily basis as they manage multiple priorities, including the privacy of their customers. We are here to protect the privacy rights of Canadians, support businesses in their efforts to comply with federal privacy law and investigate privacy complaints from individuals about businesses' privacy practices.

Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA sets ground rules for how organizations may collect, use or disclose information about individuals in the course of commercial activities. The law also gives individuals the right to see and ask for corrections to information an organization may have collected about them. If an organization's customers think the organization is not living up to its responsibilities under the law, they have the right to lodge an official complaint.

PIPEDA applies to organizations engaged in commercial activities across the country, except in provinces that have their own private sector privacy laws. Quebec, Alberta and British Columbia each have their own law, and Ontario has a law which focuses specifically on personal health information. Even in these provinces, PIPEDA continues to apply to the federally-regulated private sector and to personal information in inter-provincial and international transactions.

PIPEDA also protects employee information, but only in the federally-regulated sector. Organizations covered by the Act for their customer information may wish to consider extending the same protections to their employee information.

Personal information can include a wide range of elements, from a person's name and age to their ethnicity, medical information and income level. To find out more about what constitutes personal information or about specific privacy laws, please visit privcom.gc.ca and look under Privacy Legislation.

Getting started

IF YOU ARE READING THIS GUIDE, YOUR BUSINESS has likely designated you as the individual in charge of privacy compliance. In fact, privacy legislation requires your business to designate someone for this important task.

This document contains many important principles that will help you build a proactive and responsive privacy policy.



Look beyond this booklet

IF YOU DO THE RIGHT THING ON THE PRIVACY FRONT, your customers will appreciate it and you will avoid a privacy complaint or investigation. This guide is to help steer you in the right direction. To learn more about how to build privacy protection into your business operations, please supplement the information here by reviewing the Business Guide and the E-learning tool for retailers online under Information for Businesses, as well as other important resources, at **privcom.gc.ca**.

An airtight privacy policy is good business

PRIVATE SECTOR PRIVACY LEGISLATION REQUIRES ORGANIZATIONS TO BUILD privacy policies that outline how they collect, use and disclose their customers' personal information. That process need not be difficult. Under the heading Build Your Own Policy, below, we have compiled a checklist of actions that represent some of the key elements for compliance with the federal law. While the list is not exhaustive, it will help build the essential elements of your new privacy policy.

Collect and keep information with care

WHEN YOU COLLECT INFORMATION FROM YOUR CUSTOMERS, YOU MUST ensure that you explain your purpose and get their consent in advance. Sometimes express consent is required, while other times implied consent may be sufficient. For more information on this, read our fact sheet online entitled *Determining the appropriate form of consent under PIPEDA*. It's also important not to collect information for one purpose and then use it for another, without telling or requesting the permission of your customers.

People are understandably concerned about how you will use their information and your privacy policy will help put them at ease.

Under the law, you must also make sure that any personal information you collect is protected with adequate security safeguards.

One of the easiest and cheapest ways to make your business privacy-compliant is to only collect the personal information you actually need. If it isn't really needed for your business, don't collect it.

Another quick and easy security win is to limit who gets access to customer information on a "need-to-know basis." Make a list of those employees who really need to use customer information to do their job. If they don't need it, make sure they can't see it.

Securing personal information from prying eyes can be as simple as locking a filing cabinet or restricting who has access to an office.

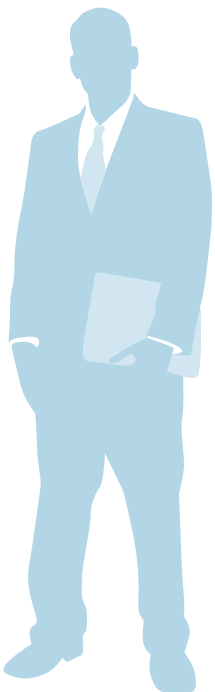
It is also important to ensure that computer systems which hold personal information are adequately protected with safeguards such as passwords, encryption and firewalls. Technologies change rapidly, so you will need to review and update security measures regularly. Retailers should also use a cash register that truncates ("x" out) payment card numbers on customer receipts.

Build your own policy



Keep it simple.

Your policy should be clear, concise and written in plain language so it is easy to understand. It should provide enough details to help your customers understand how you manage their information.





Review other privacy policies.

Online you can find policies of organizations similar to yours. Although our office does not endorse specific privacy policies, we have found that the financial services sector and telecommunications companies have mature policies worth emulating. Gain more insight into the requirements of your privacy policy by reviewing the principles in Schedule 1 of PIPEDA, which can be found online at privcom.gc.ca.



Collect only what you need.

You can collect only information that is needed for your business purposes—for example, to manage a commercial relationship and provide ongoing service, to bill and collect for products or services, to market to individuals, and to meet legal and regulatory requirements.



Be open about when personal information may be disclosed.

You must indicate in your policy if you intend to disclose customer information to an affiliate or partner organization, or any other third party. You needn't necessarily name each organization, but provide a general idea of the types of companies in question. And you must give your customers the opportunity to consent.



Tell customers when information will be stored outside of Canada.

The use of a third-party information processor, such as a company that provides payroll services, increases the likelihood that information under your control will be stored outside Canada. You must be open with your customers about this possibility.



Be open about how you safeguard information.

The risk of identity theft and other unauthorized uses of personal information is always present and ever changing. It's critical to keep the personal information in your care safe and secure. Customers and employees will appreciate your candour about how you intend to protect their information from such abuses.



Let customers know how long you will keep information.

PIPEDA requires that you keep personal information only for as long as it is needed to fulfill your purposes. If legislation such as the *Income Tax Act* authorizes you to store personal information over a long period, consider disclosing that in your privacy policy.



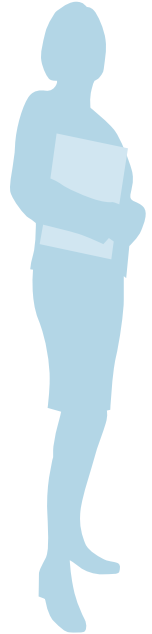
Consider employees separately.

Typically, organizations' purposes for collecting, using and disclosing employee information are to administer payroll, pension, benefit and departure provisions; to provide employee programs; to manage company property; and to hire and retain a highly skilled workforce. Because these purposes are different than those for collecting customers' information, they warrant a separate section in your privacy policy.



Make yourself available for questions.

Let individuals know how to contact your organization for privacy information, either through email or through a toll-free number. Also, tell customers they can contact the Office of the Privacy Commissioner at **1 800 282-1376** if they are unsatisfied with your response to their privacy concern.



Engaged employees will help retain customers

PRIVACY LEGISLATION REQUIRES THAT YOU EDUCATE EMPLOYEES ABOUT your organization's privacy practices and policies. It also stipulates that employees must understand their role in implementing such policies and be able to communicate them.

When you train your employees to speak openly with customers about your organization's reasons for collecting personal information—and its plans for the specific use of that information—you increase trust in your business relationships and help build pride among employees who do business on your behalf.

Below is a list of ideas to help you start an in-house training program for employees. Our checklist is only intended as a starting point. For more information about how to train employees, please review the following resources online in the Information for Businesses section at privcom.gc.ca: Guide for Businesses, E-learning tool for retailers, and PIPEDA self-assessment tool.

Although we use the terms *training program* and *refresher course*, these phrases can mean a variety of things. If your organization is small, the process of training employees may be as simple as a one-on-one conversation.





Determine which employees need the most training.

Usually, employees who deal directly with customers collect information that will elicit the most questions. They need to know when to ask for help or refer a matter to your privacy officer.



Keep key employee teams in mind.

It is tempting for marketing and product-development employees to take advantage of your customers' information as they work to improve and sell your products. Consider running short workshops for these groups so they understand your organization's policies and obligations for managing personal information appropriately.



Incorporate privacy issues into standard training programs.

If your organization is small, or has no official training program, consider organizing one around your new privacy policy—and running regular refresher courses. An online reference or printed guide to your policy is a great resource for employees learning about your policy.



Develop a process for updating privacy-policy information.

This will enable you to respond to new issues as they arise and provide ongoing updates to employees to ensure that they can respond appropriately in the circumstances.



Review customer complaints regularly.

This strategy will help you address concerns about your privacy policy and practices and enhance your privacy-training program.



Let employees know where to go for help.

While it is not possible to anticipate every question that customers will ask, providing key information and access to resources or individuals within the organization who can provide further information will go a long way to help both customers and employees understand your practices.



Develop a quiz to test employees' knowledge.

A sample quiz has been included on the back inside cover of this publication. Use or expand on it to help keep employees informed of important privacy-policy issues.

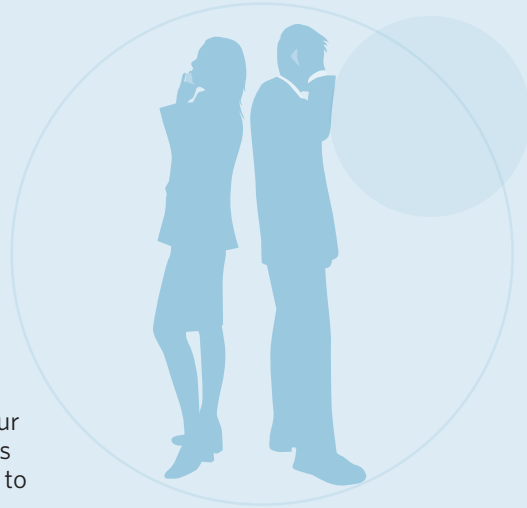


Use an honest and open approach

IT IS VITAL TO GIVE YOUR CUSTOMERS A SINGLE POINT OF CONTACT AT YOUR organization to deal with privacy issues. Many unhappy consumers have approached the Office of the Privacy Commissioner upset that they could not find someone within a business who could answer their privacy questions.

When things get difficult

NO MATTER HOW HARD YOU work at enhancing customer loyalty, there will be instances when your organization does not meet your customers' expectations of privacy. Recovering customer loyalty can be a simple process if it's done right. You can use these four steps to resolve privacy concerns before people make a complaint to our Office.



- 1. TAKE RESPONSIBILITY.**

Sincerely apologize to the customer for not meeting their expectations. Often, this is all you need to do to address the concern and maintain customer loyalty.

- 2. FIX THE PROBLEM.**

If your organization made a mistake, take action right away. If your privacy policy has been called into question, determine if the policy is appropriate and whether it should apply to similar circumstances in future.

- 3. MAKE A PEACE OFFERING.**

If your organization has made a mistake, offer your customer something meaningful for their inconvenience. If the customer wants a written apology, consider having someone in authority draft a letter.

- 4. CHECK IN WITH DISGRUNTLED CUSTOMERS.**

Follow up to ensure the issue has been resolved to your customer's satisfaction.

These steps may not resolve all your customers' privacy issues, but they will help repair damaged relations, build customer loyalty and avoid privacy investigations. Above all, ensure that your front-line staff have support from your key privacy officers to address your customers' concerns.

Educate your employees regularly

YOUR ORGANIZATION'S PRIVACY POLICY IS A CRITICAL TOOL TO SAFEGUARD your customers' personal information. It is your responsibility to ensure your employees are aware of your company's policy and the circumstances under which they may and may not collect, use or disclose customer information—and that they understand the reasons for collecting information.

Feel free to adapt the quiz below and administer it to employees at regular intervals. It will help refresh them about your privacy policy and go a long way toward building a culture of respect in your organization toward privacy issues.

Privacy Policy Quiz

1. What personal information does your organization or branch collect and why do you collect it?

2. How does this organization safeguard customers' personal information?

3. Who is the point of contact in this organization for more information about your privacy policy, to clarify the policy or to register a privacy complaint?

4. Under what circumstances does your organization disclose personal information, such as to credit agencies or collection agencies?



Office of the
Privacy Commissioner
of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP54-17/2008
ISBN 978-0-662-06051-2

For more information on private sector privacy laws in Canada, visit:

- Office of the Privacy Commissioner of Canada - privcom.gc.ca
- Commission d'accès à l'information du Québec - cai.gouv.qc.ca
- Office of the Information and Privacy Commissioner of Ontario - ipc.on.ca
- Office of the Information and Privacy Commissioner of Alberta - oipc.ab.ca
- Office of the Information and Privacy Commissioner for British Columbia - oipc.bc.ca

This guide was prepared by the Office of the Privacy Commissioner of Canada in consultation with the Office of the Information and Privacy Commissioner of Alberta.