Privacy Policy Guide for Architectural Practices

Version 1.0
September 25, 2020

Under the *Personal Information Protection and Electronic Documents Act* (PIPEDA), businesses must obtain consent for the collection, use, disclosure, and retention of personal information in the course of its commercial activities. A commercial activity is defined as any transaction, act, or conduct (or course of conduct) that is of a commercial character.

The Office of the Privacy Commissioner offers a toolkit for businesses, which is the best place to begin in your understanding of what is required under Canada's privacy law.

The OAA encourages all members and holders of a Certificate of Practice to be aware of their obligations under Canada's privacy legislation. This guideline is offered as a resource to facilitate the creation and enactment of each practice's own privacy policy where they may not yet have one, or where their existing policy may require updating. Every business—and this includes every architecture practice—must have a privacy policy.

While the OAA invites members and holders of a Certificate of Practice to use this document as a tool to facilitate writing or improving their own privacy policy, it is important every business still seek legal advice. Take time to consider the requirements your office has, the tools you use, and the different places you will want to refer to a privacy policy—your HR policies, your contracts, or your website.

Every business collects information a little differently and most use different tools to keep their records, which include personal information. However, there are common principles with which one must always comply.

The links above will take you to the Office of the Privacy Commissioner where you will always find current information. Visit the Privacy Commissioner of Canada website pages for businesses to better understand the definitions of each category listed below.

1. **ACCOUNTABILITY**
2. **IDENTIFYING PURPOSES**
3. **CONSENT**
4. **LIMITING COLLECTION**
5. **LIMITING USE, DISCLOSURE, AND RETENTION**

6. **ACCURACY**
7. **SAFEGUARDS**
8. **OPENESS**
9. **INDIVIDUAL ACCESS**
10. **CHALLENGING COMPLIANCE**

Examples for each category follow.

Example for title of a privacy policy:
[Certificate of Practice name] Privacy Policy

Example for the subtitle text in your policy:
This policy is created for [name of Certificate of Practice] activities related to the practice of architecture pursuant to the Canadian Federal Government's Personal Information Protection and Electronic Documents Act (PIPEDA)

1. ACCOUNTABILITY

You collect information about your colleagues, employees, clients, and others. You are responsible for personal information under your control.

The Certificate of Practice must designate a Privacy Officer who is responsible for compliance with your policy and the legislation. You can designate more than one Privacy Officer. There are important timelines for which a Privacy Officer is responsible, and those should be included in a procedure manual for your Privacy Officer.

Example for text in a policy:

The [name of practice] has designated [title and name] as the Privacy Officer(s). General questions and comments related to PIPEDA and the [practice/firm/practice name's] compliance with the legislation, as well as inquiries from others should be forwarded to our Privacy Officer(s) at [email].

The Privacy Officer(s) can also be contacted regarding concerns related to the business's general compliance with the legislation, including the collection, use, retention, and destruction of personal information.

[Name of Privacy Officer(s)] is/are the data protection officer(s) for the purpose of the General Data Protection Regulation.

IMPORTANT NOTE

Regardless of where your business is located, the General Data Protection Regulation (GDPR) is the European Union's (EU) Data Protection Law that you are bound by if you have personal information from people or businesses in the EU. Additional information is available at https://gdpr.eu. This may be the same as it relates to the United Kingdom's *Data Protection Act 2018*, but you should seek legal advice in this regard, especially if you have staff, projects, clients, or other relationships with the UK.

2. IDENTIFYING PURPOSES

The purpose for which personal information is collected must be identified before the time that the information is collected. Privacy policies should be available to the individuals they affect. How they are shared will vary. Each practice must decide if the information belongs on their website and how they will make it available to those most impacted.

> ***Example for text in a policy:***
>
> *Personal information is collected by the [name of business] for the purpose of enabling the practice to contact its clients, colleagues, and related services, to pay and provide benefits to its staff.*
>
> *You must be specific here. Indicate all the information you are collecting and what the purpose is.*

IMPORTANT NOTE

If you have a specific procedure for people who sign up for online newsletters or other information, or if consent for the collection and use of personal information is in your contracts, indicate that in this portion of the policy.

The Certificate of Practice's HR manual should include information about the retention and use of your staff's (current and former) personal information. If everyone in the office gets everyone else's personal contact information on an internal list, you should seek legal advice about the best way to secure consent and include this in your policy, on hiring documents, and on other appropriate documentation.

3. CONSENT

The knowledge and consent of the individual is required for the collection, use, disclosure, or retention of personal information. Get consent in writing. Even

though you have already stated the purpose for collecting the information, it is important to restate it in this section of the policy. This section deals with the importance of getting written consent. As you follow the document, you will see that you must specifically describe what the consent is for. Examples include collection of personal data for employment purposes, or collection of personal data for the purpose of providing architectural services for a project/client.

Example for text in a policy:

Personal information collected, used, disclosed, and retained by the [name of Certificate of Practice] is identified in the [consent form/contract]. The [name of Certificate of Practice] intends to collect, use, disclose, and retain personal information for the purpose of enabling [group insurance/other benefits/pension providers] to contact these individuals.

4. LIMITING COLLECTION

The collection of personal information must be limited to that which is necessary and must be collected by fair and lawful means. You cannot keep information you have not asked for permission to use. You cannot use information collected for a specific purpose for another purpose (e.g. giving your employees' or clients' names and contact information to your favourite charity for their fundraising purposes).

Example for text in a policy:

All personal information collected, used, and disclosed by the [Certificate of Practice] is obtained using the [list documents] and is limited to the purpose for which it was collected (e.g. for the purpose of enabling the [Certificate of Practice] to contact staff, clients, colleagues on current projects, interested parties, and other classes of persons).

5. LIMITING USE, DISCLOSURE, AND RETENTION

It is important to include some specific language related to:

1. How you limit the disclosure of the information you have on file;
2. How you keep that information safe;
3. How it is disclosed (i.e. with the person's consent and only for XYZ purpose);

4. The accuracy of the information kept;

5. Who is responsible for updating personal information (e.g. where it is employee information, one should indicate whether there is a specific form, or state that notice by email is acceptable); and

6. An individual's access to their files/personal information.

These issues are separate categories and should be addressed clearly whether or not you combine them in one portion of the document

Example for text in a policy:

Personal information collected by the [Certificate of Practice] in the course of its commercial activities shall not be used, disclosed, or retained for purposes other than those for which it was collected, except with the consent of the individual or business or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes, following which it shall be destroyed, erased, or anonymized.

The Certificate of Practice may disclose personal information collected in the course of its commercial activities without the knowledge or consent of the individual if:

- *the disclosure is to a lawyer and/or their insurer who represents the Certificate of Practice for the purpose of defending the Certificate of Practice against a claim made in the course of the provision of architectural services;*

- *the disclosure is to a lawyer who represents the Certificate of Practice for the purposes of collecting a debt owed to the Certificate of Practice;*

- *the disclosure is to a lawyer who represents the Certificate of Practice for the purposes of an employment law matter;*

- *the disclosure is to a lawyer who represents the Certificate of Practice in any matter related to the practice of architecture;*

- *the disclosure is required to comply with a subpoena or an order of the Court;*

- *the disclosure is to a person or body with jurisdiction to compel the production of information; or*

- *the disclosure is to an investigative body and the request for disclosure is reasonable for purposes related to investigating a breach of an agreement or contravention of the laws of Canada or a province or is required by law, and in other limited circumstances outlined in PIPEDA.*

[name of Certificate of Practice] will destroy unnecessary personal information. An individual may also request, in writing to the Privacy Officer, that their personal information be destroyed.

6. ACCURACY

The Certificate of Practice wants to ensure the information it is keeping is current and up to date. Specify how you ensure the information is correct and, where appropriate, who is responsible for updating the information.

Example for text in a policy:

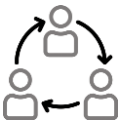
[name of Certificate of Practice] makes every effort to keep accurate and up-to-date records, but each individual is responsible for updating their contact information when it changes, if they are an employee, creditor, debtor, or someone else contractually obligated to do so.

7. SAFEGUARDS

The Certificate of Practice wants to ensure it is taking appropriate measures to protect the information it gathers. Include those measures in your policy—specify how you ensure the information is safe and, where appropriate, who is responsible for those procedures or systems.

Example for text in a policy:

[name of Certificate of Practice] will collect, use, disclose, and retain personal information and ensure the personal information is protected by security safeguards appropriate for the sensitivity of the information.



8. OPENNESS

The Certificate of Practice has to be open, and share its policies whenever they are requested. Some privacy policies should be posted publicly.

Example for text in a policy:

An individual may request information about the [name of Certificate of Practice] policies and practices relating to the management of their personal information.

9. INDIVIDUAL ACCESS

The Certificate of Practice has to give access to an individual who requests their private information.

Example for text in a policy:

An individual may request confirmation of whether the [name of Certificate of Practice] holds personal information about the individual and may request access to their personal information. Upon written request to the Privacy Officer, [name of Certificate of Practice] will provide an account of the use that has been made (or is being made) of that information, as well as an account of any third parties to which the personal information has been disclosed.

10. CHALLENGING COMPLIANCE

Anyone can address a challenge concerning compliance regarding the above nine principles with the designated Privacy Officer and/or to the Office of the Privacy Commissioner of Canada.

Example for text in a policy:

Anyone who is not satisfied with the response to their access or update request, or how your personal information is being managed is invited to contact the [name of Certificate of Practice]'s Privacy Officer at [email].

Anyone who is not satisfied with how the [name of Certificate of Practice]'s Privacy Office addressed their concern may bring the matter to the attention of the Privacy Commissioner.

DATE ADOPTED
Be sure to include the date you adopt your policy and the dates when they are updated.

The OAA gives every Certificate of Practice permission to copy any portion of this document. You are reminded to seek legal assistance specific to your needs, the systems and tools you use to store information, and the work being done by your firm. Privacy requirements in Canada are of concern to you as well as privacy requirements in other jurisdiction where you are offering or providing architectural services.