



OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Office of the Information and Privacy Commissioner

Privacy Policy

Purpose

The purpose of this document is to establish a clear privacy policy that informs employees of the Office of the Information and Privacy Commissioner (OIPC) and the public about the Commissioner's expectations with regard to the management of personal information. This policy also applies to any service providers collecting, using, or disclosing personal information on behalf of the OIPC or ORL.

Policy Statement

At the OIPC, we are committed to providing citizens with exceptional service. As providing this service involves the collection, use, and disclosure of some personal information, protecting personal information is one of our highest priorities.

We will inform citizens of why and how we collect, use, and disclose their personal information, obtain their consent where required, and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

This Privacy Policy outlines the principles and practices we will follow in protecting citizens' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of personal information and allowing our citizens to request access to, and correction of, their personal information.

This policy is built to comply with the obligations under BC's *Freedom of Information and Protection of Privacy Act* (FIPPA). FIPPA sets out the access and privacy rights of individuals as they relate to the public sector and establishes an individual's right to access records in the custody or control of public bodies, including access to one's own personal information. FIPPA also sets out the terms under which a public body can collect, use, and disclose the personal information of individuals.

Definitions

Personal Information means recorded information about an identifiable individual other than contact information.

Contact information means information that would enable an individual to be contacted at a place of business. It includes name, position name or title, business telephone number, business address, business email, or business fax number.

Privacy Officer means the individual designated responsibility for ensuring that the OIPC complies with this policy and FIPPA.

Procedures

1. Collecting personal information

1.1 Unless the purposes for collecting personal information are obvious and the applicant or complainant voluntarily provides his or her personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

1.2 We only collect applicant or complainant information that is necessary to fulfill the following purposes:

- To verify identity;
- To contact the individual with regard to a request for review or complaint;
- To open a file and process a complaint or request for review;
- To open a file and process an access request to the OIPC under FIPPA.

1.3 Examples of personal information we may collect include:

- Personal contact information (name, address, email, phone number);
- Personal information contained in records responsive to an access request, complaint, or request for correction; and
- Context-dependent personal information that may relate to any other file or investigation undertaken by this office.

2. Consent

2.1 We obtain applicant or complainant consent to collect, use, or disclose personal information (except where, as noted below, we are authorized to do so without consent).

2.2 Consent can be provided or it can be implied where the purpose for collecting, using, or disclosing the personal information would be considered obvious and the applicant or complainant voluntarily provides personal information for that purpose.

2.3 Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), applicants or complainants can withhold or withdraw their consent for the OIPC to use their personal information in certain ways. An applicant's or complainant's decision to

withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service or product. If so, we will explain the situation to assist the applicant or complainant in making the decision.

2.4 We may collect, use, or disclose personal information without the applicant's or complainant's knowledge or consent in the following limited circumstances:

- When the collection, use, or disclosure of personal information is permitted or required by law;
- When we require legal advice from a lawyer; or
- To conduct a request for review or investigate a complaint.

3. Using and disclosing personal information

3.1 We only use or disclose applicant or complainant personal information where necessary to fulfill the purposes identified at the time of collection.

3.2 We do not use or disclose applicant or complainant personal information for any additional purpose unless we obtain consent to do so or it is authorized by law.

3.3 We do not sell applicant or complainant lists or personal information to other parties.

4. Retaining personal information

4.1 If we use applicant or complainant personal information to make a decision that directly affects the applicant or complainant, we retain that personal information for at least one year so that the applicant or complainant has a reasonable opportunity to request access to it.

4.2 Subject to policy 4.1, we retain applicant or complainant personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

5. Ensuring accuracy of personal information

5.1 We make reasonable efforts to ensure that applicant or complainant personal information is accurate and complete where it may be used to make a decision that directly affects an individual or disclosed to another organization.

5.2 Applicants or complainants may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought. A request to correct personal information can be forwarded to the Privacy Officer.

5.3 If the personal information is factually inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the applicant's correction request in the file.

6. Securing personal information

6.1 We are committed to ensuring the security of applicant or complainant personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks.

6.2 The following security measures are followed to ensure that applicant or complainant personal information is appropriately protected:

- Electronic files are stored on a Local Area Network (LAN) protected by a secure firewall. User access is controlled by userID and passwords.
- A secure, encrypted, and password protected File Transfer Protocol (FTP) server is used for transmitting or receiving records containing personal information.
- Paper files are stored in a locked cabinet in a locked room in a secure building that is alarmed; access to the floor is restricted to OIPC staff.
- All staff and contractors must review this privacy policy and are accountable for following appropriate procedures for handling personal information.
- All staff are provided mandatory privacy training before handling personal information collected by the OIPC.

6.3 We use appropriate security measures when destroying personal information, such as shredding documents and deleting electronically stored information.

6.4 We continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

7. Providing access to personal information

7.1 Individuals have the right to access their personal information in the custody or under the control of the OIPC, subject to limited exceptions and scope of FIPPA.

7.2 A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. Requests can be forwarded to the Privacy Officer.

7.3 Upon request, we also tell individuals how we use their personal information and to whom it has been disclosed, if applicable.

7.4 We will respond to requests for personal information within 30 business days, or provide written notice of an extension where additional time is required to fulfill the request.

7.5 If a request is refused in full or in part, we will notify the applicant in writing, providing the reasons for refusal and the available recourse.

8. Questions and complaints

7.1 The Privacy Officer is responsible for ensuring the OIPC's compliance with this policy and FIPPA.

7.2 Applicants or complainants can direct any complaints, concerns, or questions about compliance in writing to the Privacy Officer.

7.3 The Privacy Officer may be contacted at:

oline Twiss, Deputy Commissioner/Deputy Registrar
 P.O. Box 9038, Stn Prov Govt, Victoria BC V8W 9A4
 (250) 387-5629 Fax (250) 387-1696
[oTwiss@oipc.bc.ca](mailto:otwiss@oipc.bc.ca)

ADMINISTRATIVE POLICIES AND PROCEDURES	
Office of the Information and Privacy Commissioner	
Policy: Privacy	Effective Date: March 3, 2016
Policy Number: 2.1	Date Last Reviewed/Updated: March 5, 2019