

OIPC Personal Information Inventory

The following is an inventory of all Office of the Information and Privacy Commissioner (OIPC) personal information banks, which are files of information that are retrievable by a personal identifier, such as a name or employee number. These files contain the names of applicants requesting a review, complainants, employees of public bodies and organizations, third parties, and OIPC employees.

1. Operational files

Case files stored in the electronic case tracking system and paper files in staff offices, the file room, and off-site storage include:

- a) Requests for review
- b) Complaints
- c) Requests to disregard
- d) Requests for reconsideration
- e) Inquiries
- f) Judicial review materials
- g) FOI requests
- h) Requests for information
- i) Policy issue and consultation case files
- j) Independent Investigations Office reports
- k) Breach notifications
- l) FIPPA s. 25 notifications
- m) Audit files

2. Administrative files

2.1 Electronic:

- a) All payments to staff and contractors are processed through a corporate accounting system. It contains personal information such as addresses, travel claims, and other information required to process payments to staff and contractors
- b) We use an HR system called PeopleSoft to manage staff and positions; it contains personal information such as home addresses, tax status, spouse identification, and other information we require to manage payroll and employee status.
- c) We use Microsoft Teams, which is a cloud-based, communication and collaboration application part of the Microsoft Office 365 suite available for

desktop and mobile devices. The application features bring users together through chat, meetings, calling, and file sharing, and may include all of the data the OIPC stores on its computer network. This includes vast amounts of personal information about citizens and employees. Some of it is extremely sensitive, including health information, criminal history information, child protection information, and police information.

- d) We sometimes collect personal information from staff or contractors in our email correspondence, such as leave entitlements and change in benefit status, for example.
- e) Files on the local area network (LAN):
 - i. Employees' individual HR files (letters written to employees, salary increments, performance appraisals, leave management information, etc.)
 - ii. Facilities: there is a listing of names for key job assignments.
 - iii. Information technology: contains listings and mailboxes for staff assigned emails and passwords, and distribution lists – with employees' names and where they work.
 - iv. Finance: leave liability, budget projections, and budget building spreadsheets for the purposes of informing budget projections – contains names, salaries and vacation earned.
- f) Travel vouchers: contain names and home addresses of staff.

2.2 Paper files:

- a) Historical travel vouchers: contain names and home addresses of staff, filed on and off site.
- b) Historical leave management forms: contain names and often information on sick and special leave about employees.
- c) See 2.1c) above: these documents are often printed and stored as paper files, which are maintained on and offsite.
- d) First aid incident reports: kept here on behalf of the employers. These do contain personal information.
- e) Historical HR files.

3. Purposes of collection of personal information

We collect personal information that is necessary to fulfill purposes related to our programs or activities including:

- 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 under FIPPA;
- to respond to a breach;

- to collect, use, and disclose information authorized under the LTA or FIPPA; and
- to otherwise fulfill any other duties under PIPA, FIPPA and the LTA.
- to manage OIPC employees and to onboard and offboard employees

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;
- Personal information of individuals subject to regulatory action; and
- Context-dependent personal information that may relate to any other file, investigation or work undertaken by the Offices as authorized in relation to the exercise of the powers of the Commissioner and Registrar.

ADMINISTRATIVE POLICIES AND PROCEDURES	
Office of the Information and Privacy Commissioner	
Policy: OIPC Personal Information Inventory	Effective Date: March 3, 2016
Policy Number: 2.4	Date Last Reviewed/Updated: November 25, 2024