Corporate Policy

100 Newport Drive, Port Moody, BC, V3H 5C3, Canada
Tel 604.469.4500 • Fax 604.469.4550 • www.portmoody.ca

Section:	Administration	01
Sub-Section:	Freedom of Information and Protection of Privacy	0580
Title:	Privacy Breach	2016-02

Related Policies

Number	Title
01-0580-2016-01	Privacy
A04-1490-2016-01	Working Away from the Office

Approvals

Approval Date: June 7, 2016	Resolution #: *CW16/083*
Amended: September 19, 2017	Resolution #: *RC(CW)17/031* (*CW17/117*)
Amended:	Resolution #:
Amended:	Resolution #:

Policy

The City of Port Moody (City) is committed to ensuring the protection and security of all personal information that it collects, uses, maintains, and discloses in the course of carrying out its responsibilities.

The purpose of this policy is to describe the City's process for responding to privacy breaches, and to ensure compliance with the *Freedom of Information and Protection of Privacy Act* (*FIPPA*).

Definitions

Records are broadly defined under the *FIPPA* and include any paper or electronic media which is used to store or record information. At the City, this includes all paper and electronic records, books, documents, photographs, audio or visual recordings, computer files, email, and correspondence.

Personal information is recorded information about an identifiable individual, and includes such things as an individual's name, address, birth date, personal contact information, financial information, as well as opinions and statements made about the individual.

Privacy breach is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by the *FIPPA*, and includes situations where the unauthorized activity is suspected to have taken place or where records containing personal information have been lost or stolen.

Staff means all employees, independent contractors, service providers, and volunteers employed or engaged by the City.

Procedures

All staff must immediately report actual or suspected privacy breach incidents in accordance with this Policy. If there is any question about whether a privacy breach has occurred or may occur, staff are directed to consult with the Privacy Officer.

All staff are expected to provide their full cooperation with any investigation or response to a privacy breach incident.

<u>Privacy Breach Response</u>

Step One – Duty to Report

Upon discovering or learning of a privacy breach, all staff shall:

- immediately report the privacy breach to their manager, supervisor, or Privacy Officer;
- take immediate action, where possible, to ascertain the extent of the privacy breach and to contain or stop the breach, such as by:
    - isolating or suspending the activity that led to the breach;
    - taking steps to recover personal information, records, or equipment; and
    - determining the extent of the breach, including identification of what records or personal information was involved; and

- preserve any information or evidence related to the breach for investigative purposes.

Upon discovering or being notified of an actual or suspected privacy breach, the manager or supervisor shall promptly notify the Privacy Officer, and work with the Privacy Officer to contain, investigate, and respond to the breach.

Step Two – Assessment
Upon being notified of a privacy breach, the Privacy Officer shall:

- assess what additional steps are required to contain the breach, and implement such steps as necessary;
- identify the type and sensitivity of the personal information involved in the breach, and any steps that have been taken or can be taken to minimize the harm arising from the breach;
- identify the individuals affected by the breach, or whose personal information may have been involved in the breach;
- estimate the number of affected individuals; and
- make assessments of the types of harm that may flow from the privacy breach.

The Privacy Officer shall be responsible for conducting a detailed investigation into the causes of the privacy breach and other contributing factors. The investigation shall include but not be limited to:

- assessing all information reported to the Privacy Officer;
- engaging in fact-finding to assess the causes of the privacy breach;
- considering other exacerbating factors that may have contributed to the breach or the harm flowing from the breach; and
- considering the foreseeable harm arising from the breach, including but not limited to:
    - the sensitivity of the personal information involved in the privacy breach;
    - the risk of harm to affected individuals, including identity theft, and emotional and mental harm, humiliation, and stigma;
    - risk to public safety;
    - loss of public trust in the City; and
    - financial and legal exposure.

Step Three – Notification
The Privacy Officer shall make a recommendation to the City Manager regarding whether notification of the privacy breach should be made to affected individuals or the Office of the Information and Privacy Commissioner of British Columbia (OIPC). The considerations shall include, but not be limited to:

- whether notification will help to avoid or mitigate harm to affected individuals, the City, or the public;
- provincial, federal, or other legal requirements to notify (i.e. contractual or statutory obligations);
- potential risk of identity theft or fraud flowing from the breach;

- any risk to safety or physical harm arising from the privacy breach (e.g. stalking, harassment);
- any stigma flowing from the breach for affected individuals, including risk to reputation, hurt, hurt feelings, or humiliation;
- any risk of loss to business or employment opportunities for affected individuals;
- loss of confidence or trust in the City or other public bodies; and
- any guidance documents issued by the OIPC concerning notification.

The determination about whether to provide notification of the privacy breach shall be made promptly following the breach. Any notification shall be undertaken as soon as reasonably possible. If any law enforcement agencies are involved in the privacy breach incident, then notification will be undertaken in consultation with such agencies.

Where feasible, direct notification (phone, email, letter, or in person) is preferable, but indirect notification (i.e. public announcement or media release) may be considered in appropriate circumstances depending upon the scope of the breach, the number of affected individuals, cost, effectiveness of notification methods, and other relevant factors.

Step Four – Prevention
The Privacy Officer shall report to the City on the outcome of his or her investigation, and make recommendations concerning what steps can or should be taken to prevent similar privacy breaches from occurring in the future. The City shall take appropriate action to prevent privacy breaches.

Contact Information
Questions or comments about this Policy may be addressed to the Privacy Officer at: foi@portmoody.ca.

Monitoring/Authority

The policy is to be administered and monitored by the Legislative Services Division.