Oshawa

Public Report

To:	Corporate Services Committee
From:	Sandra Kranc City Clerk David J. Potts, City Solicitor and Head, Legislative and Regulatory Directorate
Report Number:	CORP-14-77
Date of Report:	June 12, 2014
Date of Meeting:	June 16, 2014
Subject:	Privacy Breach Protocol
File:	A-3410

1.0 Purpose

The purpose of this report is to present a privacy breach protocol for approval by City Council.

2.0 Recommendation

That the Corporate Services Committee recommend to City Council:

That the Privacy Breach Protocol appended as Attachment One to Report CORP-14-77 dated May 22, 2014 be adopted.

3.0 Executive Summary

The Municipal Freedom of Information and Protection of Privacy Act (the Act) governs, amongst other things, the collection, use and disclosure of personal information by government institutions. Municipalities are prohibited from disclosing personal information in their custody and control except in several specific circumstances. A privacy breach occurs when personal information is collected, retained, used or disclosed in contravention of the Act. Privacy breaches may occur in a number of different ways. For instance, they may emerge from the intentional and deliberate actions of an individual, or the inadvertent failure of existing processes or systems. As a best practice, the Information and Privacy Commissioner of Ontario has recommended that institutions establish a protocol to mitigate and investigate a suspected privacy breach. The proposed Privacy Breach Protocol has been developed to respond to the City's obligations under the Act and to provide a coordinated approach when acting in response to an alleged privacy breach.

4.0 Input From Other Sources

- City Manager
- Legal Services

5.0 Analysis

5.1 Legislative Overview

The Municipal Freedom of Information and Protection of Privacy Act provides individuals with a right to access information in the custody and control of the City, subject to several limited and specific exemptions. Additionally, it establishes a set of rules intended to protect the privacy of individuals and the personal information they entrust with the City.

Personal information is broadly defined in Section 2 of the Act and the following are the most common types of personal information collected and maintained by the City:

- the name, address, telephone number, email address, age and gender of an individual;
- information respecting an individual's employment, medical, criminal and educational history;
- a record of financial transactions in which an individual has been involved; and,
- the personal opinions of the individual, except where they concern another individual.

The Act and the obligation to protect an individual's personal privacy applies to all individuals employed by or acting on behalf of the City, including members of Council, agents, contractors and volunteers.

To protect an individual's right to privacy, the Act governs how the City may collect, retain, use and disclose personal information which is necessary for the delivery of various City programs and initiatives.

5.2 What Constitutes a Privacy Breach?

Where the City collects, retains, uses or discloses personal information in a manner that is inconsistent with the Act it is considered an alleged privacy breach for which the City has an obligation to investigate and, where possible, remedy.

Although privacy breaches may be the result of a deliberate action on the part of an individual or group within the organization, they may also result from the unintentional failure of systems, processes and policies.

To demonstrate, the following scenarios are some examples of situations that could each constitute a privacy breach:

- Releasing the name, address or other personal information of an individual who has submitted a complaint alleging a violation of the City's by-laws;
- Misplacing a USB drive containing tax billing information;
- Sharing with members of the public, without the consent of the individual, the educational, or employment history of an individual applying for a position on an advisory committee of Council;
- Inadvertently delivering personal and confidential correspondence to an individual to whom it is not addressed;
- Compiling a history of financial transactions conducted by an individual with various City departments;
- Using information contained on the Voters' List to facilitate the collection of debts owed to the City;
- Disclosing video surveillance footage to law enforcement agencies where the footage is not required to support a law enforcement proceeding or where a law enforcement proceeding is likely to result; and
- Placing records containing personal information into the garbage or recycling.

5.3 Recent Examples

Although the Act does not require an institution to report suspected or confirmed privacy breaches, recent examples highlight the fact that privacy breaches occur and with potential reputational or financial harm to the organizations involved.

- In June 2007, the Information and Privacy Commissioner of Ontario was alerted by a member of the media to the placement of unshredded records containing personal information in clear plastic bags for recycling outside of the Old City Hall Courthouse in Toronto. The Commissioner's investigation determined that the disposal of some of the information was not in accordance with the Act and represented a privacy breach.

- In December 2009, a nurse employed by Durham Region lost an unencrypted USB drive containing, amongst other things, the name, phone number, date of birth and health card number of more than 83,000 individuals vaccinated against H1N1. A class action was launched against the Region and settled in 2012 for $500,000 plus additional costs for those individuals who can prove they suffered financial losses as a direct result of the lost USB drive.

- In January 2013, Human Resources and Skills Development Canada lost a portable hard drive containing the names, social insurance numbers, dates of birth, contact information and loan balances of more than 583,000 Canada Student Loan borrowers. A class action suit was certified on March 17, 2014 and remains before the courts.

- On June 5, 2014 it was announced that a significant privacy breach occurred at Rouge Valley Centenary, a hospital in Scarborough, where two hospital employees sold to private firms marketing Registered Education Savings Plans, the name, address and telephone number of more than 8,300 patients, namely mothers who delivered children at the hospital. An investigation into the breach is currently being conducted by the Information and Privacy Commissioner of Ontario.

In recognition that these events occur, either through the deliberate actions of an individual, or the failure of policies and procedures, it is important that an organization have an effective breach management process in place to respond.

5.4 The Protocol

Consistent with privacy best practices, in every instance, the protocol outlines a five step process that shall guide the City's response to a suspected privacy breach.

The protocol is implemented when an agent, contractor, volunteer, member of Council or staff member suspects that a privacy breach has occurred.

Where a breach is thought to have occurred, staff are to identify, where possible, the suspected source of the personal information, and immediately notify their supervisor. In turn, the supervisor will notify the City Clerk or Manager, Records Information Systems within one business day.

Once received, the City Clerk or Manager, Records Information Systems will:

1. implement containment strategies focused on mitigating the scope of the breach; and,

2. establish a response team with representation from City Clerk Services, Legal Services, the Branch or Section where the suspected breach occurred and any other areas deemed appropriate.

The response team will conduct a meeting or teleconference as soon as practicable to develop a more fulsome containment strategy taking into consideration the following:

- The location and date of incident and discovery;
- The cause of the incident, if known;
- An estimate of the number of individuals involved;
- The type of individuals affected by the breach (e.g. internal vs. external);
- The types of personal information involved;

- Any identifiable records associated with the breach;
- Any actions already undertaken to contain the breach; and,
- Any other organizations who have been notified (e.g. police)

As noted, containment strategies will commence immediately in order to mitigate the scope of the suspected breach. Working in cooperation with the area manager and staff, City Clerk Services and other areas where appropriate will undertake the following actions:

- Retrieve and secure any records containing personal information, or otherwise associated with the suspected breach;
- Where appropriate, isolate and/or suspend access to any system associated with the suspected breach
- Suspend all processes or practices which are believed to have served as a source for the suspected breach;
- Take any other actions necessary to contain the suspected breach.

City Clerk Services shall advise the Information and Privacy Commissioner of Ontario of all suspected privacy breaches and all individuals affected by a potential privacy breach.

After containing and notifying the affected individuals, City Clerk Services, with assistance from the response team, will conduct an investigation into the suspected or confirmed privacy breach. The investigation will establish, amongst other things:

- whether a privacy breach occurred;
- the source of the breach, including the policies, procedures or systems responsible;
- the nature and sensitivity of the personal information disclosed;
- the number and type of individuals affected; and,
- any other factors relevant to the suspected or confirmed privacy breach.

After the investigation is complete, a report shall be prepared by the City Clerk and/or Manager, Records Information Systems outlining the results of the investigation and any recommendations intended to mitigate the occurrence of future incidents.

A copy of the report shall be provided to the Information and Privacy Commissioner of Ontario, each individual affected by the suspected or confirmed privacy breach, and included on the agenda of the appropriate standing committee of Council where more than five individuals are affected, or in the opinion of the City Clerk, in consultation with the City Manager, it is determined that it is in the public interest to provide such a report.

Where recommendations are included in the report, they shall be added to the respective Branch work plan for review and, where appropriate, implemented.

6.0 Financial Implications

There are no financial implications associated with this report or the Privacy Breach Protocol.

7.0 Relationship to the Oshawa Strategic Plan

This report and the adoption of the proposed Privacy Breach Protocol support the themes of open, transparent and accountable government outlined in the Oshawa Strategic Plan.

Sandra Kranc, City Clerk

David J. Potts, City Solicitor and Head,
Legislative and Regulatory Directorate

DJP/SK/JM

File: A-3410

Privacy Breach Protocol

1. Purpose

All City of Oshawa employees and members of City Council shall, at all times, comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act*.

This protocol affirms the City of Oshawa's obligation to protect personal information in the custody or control of the institution. Privacy Breaches undermine public trust in an institution and may result in significant harm to the City and to those whose personal information is collected, used or disclosed inappropriately.

This protocol requires the immediate reporting of all Privacy Breaches and alleged Privacy Breaches to the City Clerk or Manager, Records Information Systems and outlines the steps that shall be followed when an alleged Privacy Breach is reported. This process will ensure that when an alleged Privacy Breach is discovered, it is quickly contained and investigated to mitigate the potential for further dissemination of personal information. Furthermore, the investigation shall recommend remedial steps focused on preventing similar events in the future.

2. Sources

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56

Privacy Breach Protocol: Guidelines for Government Organizations, Information and Privacy Commissioner/Ontario

3. Scope

This protocol applies to all City of Oshawa employees, volunteers, agents, contractors and members of City Council.

4. Definitions

Act – means the *Municipal Freedom of Information and Protection of Privacy Act,* R.S.O 1990, Chapter M.56

IPC – means the Information and Privacy Commissioner/Ontario

Personal Information – means recorded information about an identifiable individual, including:

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except if they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual

Privacy Breach – means the use or disclosure of Personal Information or records containing Personal Information in violation of Sections 31 or 32 of the Act

Record – means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes any Record as defined by Section 2(1) of the Act

5. Procedure

When a Privacy Breach is alleged to have occurred, City staff shall undertake immediate action. In all instances of a Privacy Breach or alleged breach, the following steps, conducted in quick succession, or concurrently, shall be followed:

Step 1: Identify and Alert

Identify the suspected source of the alleged Privacy Breach; for instance, the Records, systems or websites which are believed to have been the source of the potential Privacy Breach and alert a supervisor or manager within the area of the alleged Privacy Breach.

The supervisor or manager shall notify the City Clerk and/or Manager, Records Information Systems within one business day. If a supervisor or manager is unavailable, staff should contact the City Clerk and/or Manager, Records Information Systems directly and advise of the alleged Privacy Breach.

Upon receipt of notification, the City Clerk or Manager, Records Information Systems will establish a response team with representation from the following areas to manage the City's response to the alleged Privacy Breach:

- City Clerk Services
- Legal Services
- Branch or Section where the alleged breach occurred
- other areas where appropriate

A meeting or teleconference involving the members of the response team shall occur as soon as practicable after notice is provided to City Clerk Services of the alleged Privacy Breach. During this meeting, the response team will attempt to establish the particulars of the incident, including:

- the location and date of incident and discovery
- the cause of the incident, if known
- an estimate of the number of individuals involved
- the type of individuals involved (e.g. internal vs. external)
- the type of Personal Information subject to the breach
- any identifiable Records associated with the alleged breach
- any actions already undertaken to contain the breach
- other organizations who have been notified (e.g. police)

This information will be used to develop a containment strategy and notify the affected individuals.

After the initial meeting, the City Clerk or Manager, Records Information Systems shall advise the City Manager of the known circumstances and provide updates as appropriate throughout the process.

Step 2: Contain

City Clerk Services staff shall, in cooperation with the area manager and staff and other areas as appropriate, undertake the following actions to contain the alleged Privacy Breach:

- retrieve and secure any Records associated with the alleged breach;
- where appropriate and depending on circumstances, isolate and suspend access to any system associated with the alleged breach;
- suspend all processes or practices which are believed to have served as a source for the alleged breach;
- take any other action necessary to contain the alleged breach.

Step 3: Notify

City Clerk Services shall notify the IPC of all alleged and confirmed Privacy Breaches.

City Clerk Services shall also be responsible for notifying all individuals affected by a Privacy Breach. This notification will include information surrounding the nature of the alleged, or confirmed, Privacy Breach, the details of the breach, as understood at the time of notification, the specific personal information affected and contact information for a City representative and the Information and Privacy Commissioner of Ontario, should they have questions.

City Clerk Services shall handle all inquiries with respect to Privacy Breaches and the actions of the institution in response to an alleged or confirmed breach.

Step 4: Investigate

After using its best efforts to contain the alleged Privacy Breach and notifying the affected individuals, City Clerk Services shall undertake an investigation in an attempt to establish:

- whether a Privacy Breach occurred;
- a chronology;
- the source of the breach, including the policies or procedures responsible;
- the nature and sensitivity of the Personal Information disclosed;
- the number of individuals affected;
- the individuals or category of individuals who were affected; and
- any other factors relevant to the circumstances.

The investigation will review existing policies and procedures governing the protection of Personal Information and make recommendations intended to strengthen the protection of such information collected and used in the area.

Step 5: Report and Follow-Up

After completing the investigation, a report shall be prepared by the City Clerk and/or Manager, Records Information Systems outlining the results of the investigation, including any recommendations to mitigate future incidents. Consistent with privacy best practices, a copy of the report shall be forwarded to the IPC, as well as to all individuals who were affected by the Privacy Breach.

To uphold the principles of transparency and accountability, the report shall also be included on the agenda of the appropriate standing committee of Council where:

- more than five (5) individuals are affected by a confirmed breach; or,
- in the opinion of the City Clerk, in consultation with the City Manager, it is determined that it is in the public interest to provide such a report.

Recommendations from the report shall be added to the appropriate Branch work plan for review and, where appropriate, implementation.