Corporate Policy

Title:	**Privacy Breach Response Policy**
Number:	GOV-14-01
Approved By:	City Council
Administered By:	Legislative Services
Effective Date:	2014
Revision Date(s):	June 2021

1.0 Purpose/Background

The Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 ("M.F.I.P.P.A.") establishes rules for government organizations to follow to ensure the protection of Personal Information.

A Privacy Breach is any unauthorized Collection, Use or Disclosure of Personal Information in contravention of M.F.I.P.P.A.. Under the legislation, and in accordance with City policies, the City of Oshawa ("City") is responsible for ensuring that all forms of Personal Information in its Custody and/or Control are properly safeguarded from those not entitled to have access to it.

However, the City recognizes that Privacy Breaches do occasionally occur, and strives to be prepared by implementing the Privacy Breach Response Policy and Procedure, tracking Privacy Breaches and their causes, and identifying patterns and trends to inform positive change and corrective actions.

The objectives of this Policy are to:

- Establish investigation and reporting processes for Privacy Breaches;
- Ensure compliance with privacy legislation and related City policies; and,
- Establish roles and responsibilities for managing privacy investigations.

2.0 Policy Statement

City of Oshawa Employees (including employees of the Oshawa Senior Community Centres), Volunteers, Students, Agents and/or Contracted Service Providers of the Corporation of the City of Oshawa; as well as Members of all committees and boards, and Members of Council shall comply with the privacy protection requirements as mandated by M.F.I.P.P.A.

This Policy confirms the City's obligation to protect all Personal Information in the Custody and/or Control of the institution. It outlines the immediate actions that must be undertaken whenever a Privacy Breach is reported, to allow for a prompt, reasonable and coordinated response.

Privacy Breaches undermine public trust in an institution, and may result in harm to the City and to those Affected Parties whose Personal Information has been collected, used, disclosed and/or disposed of inappropriately. As such, the Policy will ensure that when a Privacy Breach is discovered it is quickly contained and investigated to mitigate the potential for further dissemination of Personal Information. It shall also allow recommendations regarding remedial steps focused on preventing similar events in the future.

3.0 Scope/Application

This Policy applies to all Employees (including employees of the Oshawa Senior Community Centres), Volunteers, Students, Agents and/or Contracted Service Providers of the Corporation of the City of Oshawa; as well as Members of all committees and boards and Members of Oshawa City Council. It also applies to all Personal Information in the Custody and/or under the Control of the City.

This Policy shall be interpreted in a manner that is consistent with the City's obligations under M.F.I.P.P.A. and the City's Access and Privacy Policy.

4.0 Definitions

Act refers to the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56, as amended.

Affected Party means any person, group of persons or organization whose interest might be affected by Disclosure. Where the affected party is an individual their right may, in some cases, be exercised by another person. Also referred to as "third party".

Agent means an individual or corporate entity representing the City of Oshawa during a business transaction (e.g. legal representation, real estate transactions, etc.).

Branch means any grouping of City of Oshawa Employees who are part of an outlet of the organization that does not constitute a separate entity but is responsible for a type of work.

Collection means the collection of Personal Information from or about the individual to whom the information relates, including unintended or unprompted receipt.

Contracted Service Provider means an individual or business that undertakes a contract or agreement with the City in order to perform a service on a continuing basis (e.g. Security Guard Services, Marriage Officiants, etc.).

Control means contents of the Record as it relates to City Business and the City's power or authority to make a decision about the Use or Disclosure of its Records.

Custody means the storage, preservation, or security of a Record for a legitimate business purpose, wherein the City could obtain a copy of the Record upon request. While physical possession of a Record may not always constitute custody, it is the best evidence of custody.

City means the Corporation of the City of Oshawa.

City Business means a core, central or basic function of the City, as related to the City's mandate and functions.

Consistent Purpose means Personal Information collected by the City that is used for the purpose for which it was collected or similar consistent purposes when carrying out City Business. The individual to whom the information relates might reasonably expect the Use/Disclosure of their Personal Information for those consistent purposes.

Council means Oshawa City Council as a whole.

Council Member means an individual member of Council, including the Mayor.

Data means information that is stored in or used by an electronic device or computer. Data includes but is not limited to information collected for research or information included in an email.

Disclosure means the release of Personal Information by any method (e.g. sharing information by any means such as verbally, sending an email, posting online) to any entity or person.

Disposition means the Destruction of Records, the transfer of historically significant Records to an Archive, or the transfer of Records to another authority.

Destruction means the physical or electronic disposal of Records or Data by means of shredding, recycling, deletion or overwriting. This also includes the destruction of Records or Data residing on computers and electronic devices supplied or paid for by the City.

Employee means all full-time, part-time, temporary and seasonal staff of the City of Oshawa including staff hired on a contract basis for a defined period of time and Students.

I.P.C. means the Information and Privacy Commissioner of Ontario. The Commissioner is appointed by the Lieutenant Governor in Council, and is independent of the government. The I.P.C. is responsible for adjudicating and issuing binding orders related to appeals, conducting privacy investigations, and has powers relating to the protection of personal privacy.

Members means a member of any committee or board which reports to, or on behalf of, the City of Oshawa, including, but not limited to, Advisory Committees, Committee of Adjustment and Oshawa Senior Community Centres (OSCC55+).

M.F.I.P.P.A. means the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56, as amended.

Personal Information means "recorded information about an identifiable individual," as defined in Section 2(1) of the Municipal Freedom of Information Protection of Privacy Act 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 unauthorized Use or Disclosure of Personal Information, including it being stolen, lost or accessed by unauthorized persons, in contravention of the privacy policies, procedures or practices implemented by the City, or agreements that the City has entered into with external Contracted Services Providers.

Privacy Incident means circumstances where there is a contravention of the privacy policies, procedures or practices implemented by the City, or agreements that the City has entered into with external Contracted Service Providers, where this contravention does not result in unauthorized Collection, Use, Disclosure and/or Destruction of Personal Information, or constitute non-compliance with applicable legislation. A Privacy Incident may also be a suspected Privacy Breach.

Record means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise as defined in section 2(1) of the Municipal Freedom of Information and Protection of Privacy Act, and includes,

(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and,

(b) subject to the regulations, any record that is capable of being produced from a machine readable record under the Control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution ("document").

Retention means the keeping and maintaining of information in the Custody or Control of the City.

Students means an individual at least 15 years of age and registered in an educational program at a high school, college or university level.

Use means to take, hold, or deploy as a means of accomplishing a purpose or achieving a result.

Volunteer means an individual who volunteers their services, from time to time, to assist in areas of the City.

5.0 Responsibilities

5.1 City Clerk

The City Clerk has responsibility for administrative duties for purposes of M.F.I.P.P.A.. Many of the duties in relation to this Policy have been assigned to the Information, Access and Privacy Officer; however, the City Clerk remains accountable for actions taken regarding the handling of Personal Information under M.F.I.P.P.A..

In relation to this Policy, the City Clerk or designate shall:

- Develop and implement standards, guidelines, policies, procedures, programs and services for the management and protection of Personal Information;
- Review Branch and departmental practices for the Collection, Use, Disclosure and Destruction of Personal Information;
- Coordinate the response to formal complaints to the I.P.C. regarding the misuse of Personal Information;
- Coordinate and lead the Privacy Breach Response;
- As required and depending on the nature or seriousness of the Privacy Breach, lead meetings and activities of the Privacy Breach Response Team;
- Determine whether and when the I.P.C. should be notified of the Privacy Breach, and if so, carry out such notification;
- Make recommendations for the prevention of future Privacy Breaches, including without limitation: Employee training, creating additional restrictions for access to Personal Information, strengthening existing methods of protection of Personal Information, review of policies, procedures, practices, and any other remedial action;
- Brief the City's Corporate Leadership Team regarding Privacy Breaches, as necessary and appropriate;
- Review internal investigation reports and monitor the implementation of all recommended remedial action(s); and,
- Ensure that Affected Parties whose Personal Information has been compromised are informed, as required.

5.2 Information Access and Privacy Officer

The Information Access and Privacy Officer is responsible for the daily administration of M.F.I.P.P.A. as related to this Policy, including undertaking any of the duties listed above, as directed by the City Clerk.

In relation to this Policy, the Information Access and Privacy Officer shall:

- Maintain a thorough knowledge of this Policy;
- Assist the City Clerk in coordinating and leading the Privacy Breach Response;

- Ensure that the Policy is fully implemented in response to Privacy Breaches, and make recommendations for remedial action(s);
- Report to the City's Corporate Leadership Team, as appropriate;
- Report the Privacy Breach to the I.P.C., as directed by the City Clerk;
- Keep track of Privacy Breaches and details of responses;
- Notify Affected Parties whose Personal Information has been compromised, as required;
- Promote changes in practice that mitigate the risk of future Privacy Breaches, and monitor the implementation of the changes; and,
- Complete any other tasks as assigned by the City Clerk in relation to the Privacy Breach Response Policy and Procedure.

5.3 City Solicitor

The City Solicitor or designate may be required to assist the City Clerk or designate, as a member of the Privacy Breach Response Team. Additionally, the City Solicitor or designate shall be required to represent the City if a Privacy Complaint or Privacy Breach is escalated to legal proceeding.

5.4 Employees, Volunteers, Students and Agents

Employees, Volunteers, Students and Agents that collect, Use, disclose and/or dispose of Personal Information for the City shall be held accountable for any actions they take with that information.

In relation to this Policy, all Employees, Volunteers, Students and Agents shall:

- Immediately report any suspected Privacy Breach to their direct Supervisor and/or Manager, or in their absence, to the City Clerk or designate;
- Participate in training regarding the appropriate handling of Personal Information in executing their duties, as provided by City Clerk Services;
- Be aware of the responsibilities as noted in City policies;
- Comply with M.F.I.P.P.A. as it governs the Collection, Use, Disclosure and Destruction of Personal Information under their Control;
- Assist with containment of the Privacy Breach by suspending the process that has caused it, as appropriate; and,
- Cooperate fully and promptly with the City Clerk or designate in the investigation and remediation of the Privacy Breach.

5.5 Supervisors/Managers

In relation to this Policy, all Supervisors and/or Managers shall:

- Immediately document the details of the suspected Privacy Breach using the Privacy Breach Report Form (Appendix 1), and submit to the City Clerk or designate, copying the responsible Director and/or Commissioner, as appropriate;
- Provide a copy of the Personal Information involved in the Privacy Breach, or a detailed description of such information to the City Clerk or designate;
- Cooperate with the City Clerk or designate, to undertake all appropriate actions required to contain the Privacy Breach;
- Cooperate fully and promptly with the City Clerk or designate in the investigation and remediation of the Privacy Breach;
- Address the conduct of the Employee, Contracted Service Provider or other Agent responsible for the Privacy Breach, in accordance with any applicable collective agreements, terms and conditions of employment or other contractual relationship, or City Policy; and,
- Ensure details of the Privacy Breach and any corrective actions are documented.

5.6 Contracted Service Providers

Contracted Service Providers shall ensure compliance with the privacy and security requirements defined in all contracts and/or service agreements with the City. Contracted Service Providers are also required to inform the City of all Privacy Breaches.

In relation to this Policy, Contracted Service Providers shall:

- Inform the City Clerk or designate immediately upon discovering a Privacy Breach;
- Take all necessary actions to contain the Privacy Breach as directed by the City Clerk or designate;
- The City Clerk or designate will complete the Privacy Breach Report Form on behalf of Contracted Service Providers, for record-keeping purposes;
- Document how the Privacy Breach was discovered, what containment actions were taken and report back to the City Clerk or designate;
- Undertake an assessment of the Privacy Breach in accordance with any applicable contractual obligations; and,
- Implement remedial action(s) to decrease the risk of future Privacy Breaches involving information under the Custody and/or Control of the City, as appropriate.

5.7 Members of Council

Council Members who have received access to Personal Information in the performance of their duties have a responsibility to protect this information while it is in their possession. Council Members must ensure that the privacy of the individual to whom the information relates is protected at all times, and must keep the information physically secure to avoid unauthorized Disclosure or Destruction.

In relation to this Policy, Members of Council shall:

- Immediately document the details of a Privacy Breach using the Privacy Breach Report Form, and submit to the City Clerk or designate;
- Provide a copy of the Personal Information involved in the Privacy Breach, or a detailed description of such information to the City Clerk or designate;
- The City Clerk or designate will complete the Privacy Breach Report Form on behalf of Members of Council, for record-keeping purposes;
- Cooperate with the City Clerk or designate, to undertake all appropriate actions required to contain the Privacy Breach;
- Cooperate fully and expeditiously with the City Clerk or designate in the investigation and remediation of the Privacy Breach; and,
- Implement remedial action(s) to decrease the risk of future Privacy Breaches involving information under the Custody and/or Control of the City, as appropriate.

5.8 Members of Committees and Boards

Members who have received access to Personal Information in the performance of their duties have a responsibility to protect this information while it is in their possession.

In relation to this Policy, Members of Committees and Boards shall:

- Immediately document the details of a Privacy Breach using the Privacy Breach Report Form, and submit to the City Clerk or designate;
- Provide a copy of the Personal Information involved in the Privacy Breach, or a detailed description of such information to the City Clerk or designate;
- The City Clerk or designate will complete the Privacy Breach Report Form on behalf of Members of Committees and Boards, for record-keeping purposes;
- Cooperate with the City Clerk or designate, to undertake all appropriate actions required to contain the Privacy Breach;
- Cooperate fully and expeditiously with the City Clerk or designate in the investigation and remediation of the Privacy Breach; and,
- Implement remedial action(s) to decrease the risk of future Privacy Breaches involving information under the Custody and/or Control of the City, as appropriate.

5.9 Privacy Breach Response Team

The City Clerk or designate will determine when to convene the Privacy Breach Response Team ("Response Team"). Typically, the Response Team is convened in the event of a large-scale or complex Privacy Breach, as determined by the City Clerk or designate.

The Response Team has two purposes:

(1) To prepare for implementation of the Privacy Breach Response Policy; and

(2) To assist and support the City Clerk or designate in the implementation of the Privacy Breach Response Policy.

The Response Team shall include pre-identified representatives from City Clerk Services, Legal Services, and any additional Branches as affected by the Privacy Breach.

The City Clerk or designate may choose to convene a meeting of the Response Team as frequently as necessary for the following purposes, or for any other relevant purpose:

- To ensure that members of the Response Team understand their roles and responsibilities;
- To review the Privacy Breach Response Policy and Procedure in order to consider whether it is in need of revision, and formulate recommendations for any such revisions;
- To verify whether any Contracted Service Providers who may have provided services in support of past Privacy Breach response efforts have adequately fulfilled the City's needs, and if necessary identify other potential consultants, experts or contractors who may be retained in the event of future Privacy Breach response efforts;
- To simulate the implementation of the Privacy Breach Response Policy and Procedure in response to different types of Privacy Breaches; and,
- To undertake such other preparatory activities as the Response Team may consider advisable from time to time.

6.0 Privacy Breach Management

Personal Information

The City is responsible for all Personal Information that is collected, retained, used, disclosed, and/or disposed of in the course of conducting City Business.

Privacy Incidents

A Privacy Incident includes:

- A suspected contravention of the privacy policies, procedures or practices implemented by the City, where this contravention may not result in non-compliance with applicable legislation;

- A contravention of agreements that the City enters into with external Contracted Service Providers, where this contravention may not constitute non-compliance with applicable legislation; or,

- A suspected Privacy Breach.

All Privacy Incidents shall be investigated in the same manner as Privacy Breaches, but may not result in the same remedial actions and notification processes, as described below.

Privacy Breaches

A Privacy Breach includes:

- The Collection, Use, Disclosure, and/or Destruction of Personal Information that is not in compliance with M.F.I.P.P.A.; and

- Circumstances where Personal Information is stolen, lost, misplaced, or subject to any other form of unauthorized or inappropriate Collection, Use or Disclosure, copying, modification, Retention and/or Destruction.

All Privacy Breaches involving the unauthorized Collection, Retention, Use, Disclosure copying, modification, and/or Destruction of Personal Information not in accordance with M.F.I.P.P.A. or corporate policies, must be immediately contained to a reasonable standard, and reported as described below.

7.0 Procedure

M.F.I.P.P.A. sets out rules that municipalities must follow when collecting, using, disclosing, retaining, and/or disposing of Personal Information. It also balances the right of individuals to privacy with the legitimate needs of City Employees (including employees of the Oshawa Senior Community Centres), Volunteers, Students, Agents and/or Contracted Service Providers; as well as Members of all committees and boards, and Members of Council to collect, Use and share information as required to conduct their work.

Whenever a Privacy Breach occurs, the timely containment of the affected Personal Information, and the rapid completion of remedial actions are essential to minimizing the harm to Affected Parties, while simultaneously demonstrating accountability and restoring trust.

If a Privacy Breach is suspected to have occurred, individuals must take immediate action. In all instances of a Privacy Breach or Privacy Incident, the following steps conducted in quick succession, or concurrently, must be followed.

Step 1: Contain the Privacy Breach

Immediately upon identification of a Privacy Incident or Breach, Supervisors and/or Managers with the assistance of all involved in the Privacy Incident or Breach, shall identify the nature and scope of the Privacy Incident or Breach and take any necessary actions to contain it.

Examples of containment activities may include:

- Retrieving and securing any Records and Personal Information that may have been disclosed (in either hard copy or electronic);
- Ensuring that no Personal Information has been retained by an unauthorized recipient and retrieve contact information in case follow-up is required;
- Suspending the practice or process that resulted in the Privacy Incident or Breach;
- Shutting down the information system that was potentially breached;
- Revoking access temporarily, or permanently, to the affected system;
- Contacting a Law Enforcement Agency, as appropriate (e.g. if the Privacy Incident or Breach involves theft or other criminal activity); and/or,
- Any other action necessary to contain the Privacy Incident or Breach.

All Privacy Incidents and Breaches must be contained immediately upon discovery. Immediate containment of Privacy Incidents will prevent them from becoming Privacy Breaches, and immediate containment of Privacy Breaches will prevent further unauthorized Collection, Use and/or Disclosure of Personal Information.

If it is suspected that an Employee intentionally breached Personal Information in contravention of the City's Employee Code of Conduct, the occurrence must be immediately escalated to Human Resource Services. Human Resource Services may conduct further investigations into any suspected wrongdoing, which may result in disciplinary action, as appropriate.

Step 2: Notify the City Clerk

Individuals are required to report all Privacy Incidents and Breaches to their immediate Supervisor and/or Manager immediately upon discovery. If a Supervisor and/or Manager is unavailable, Employees should contact the City Clerk or designate directly to notify them of the Privacy Incident or Breach. Members of Council are required to report all Privacy Incidents and Breaches to the City Clerk.

The responsible Supervisor and/or Manager will document all information related to the Privacy Incident or Breach on the Privacy Breach Report Form.

A copy of the Personal Information that is the subject of the Privacy Incident or Breach, or a detailed description of such Personal Information, must accompany the Form submission. The Supervisor and/or Manager shall submit the completed Form to the City Clerk or designate, copying the responsible Director and/or Commissioner, as soon as possible after the Privacy Incident or Breach has been identified.

Upon receipt of a completed Privacy Breach Report Form, the City Clerk or designate, will evaluate the risks, determine if a Privacy Breach occurred, conduct an Investigation, and may choose to convene a meeting of the Privacy Breach Response Team to manage the City's response to the Privacy Breach.

Step 3: Evaluate the Risks

The City Clerk or designate, shall evaluate the risk of the exposure and identify the cause of the Privacy Breach:

- Evaluate the nature of the Personal Information at issue; and
- Conduct an assessment of the risks associated with the Disclosure of the affected Personal Information.

An assessment of risk should encompass a review of the following:

- Risk of identity theft;
- Risk of physical harm;
- Risk of harm, humiliation or damage to reputation; and,
- Legislative requirements.

The Risk Assessment Chart (Appendix 2) may be used by the City Clerk or designate, to determine if a Privacy Breach occurred. If a Privacy Breach is confirmed, the City Clerk or designate, will evaluate the severity of the Privacy Breach and proceed in accordance with the steps below.

Step 4: Conduct an Investigation

The City Clerk or designate, will conduct an investigation into the Privacy Breach. During the investigation process, the City Clerk or designate may request the attendance of the individuals involved in the breach, their Supervisor and/or Manager/ Members of the Corporate Leadership Team involved in the Privacy Breach at an information-gathering meeting.

The investigation will assist the City Clerk or designate to:

- Review the events that led to the Privacy Breach;
- Evaluate the risk of the exposure as related to the affected Personal Information;
- Determine if the Privacy Breach was benign (e.g. human error, accidental) or malicious (e.g. deliberate sabotage, hacking);
- Determine if it was a systemic issue (e.g. network security failure), or an isolated incident (e.g. lost folder);
- Determine who was affected by the Privacy Breach and how many were affected, what types of Personal Information were involved and how sensitive it is (e.g. email address vs. financial or health information);
- Determine if the affected Personal Information could be used for fraudulent or otherwise harmful purposes (e.g. identity theft, access to system/devices, public humiliation);

- Identify who had unauthorized or inappropriate access to the Personal Information;
- Evaluate the effectiveness of the containment activities;
- Determine if any other institutions need to be contacted (e.g. Durham Region Health Department, Durham Region Police Service, etc.);
- Take note of any other factors relevant to the circumstances; and,
- Keep an ongoing Record of events as they unfold.

At the sole discretion of the City Clerk or designate, a meeting of the Privacy Breach Response Team may occur shortly after a Privacy Breach has been identified. During this meeting, the Response Team shall develop a response strategy, as appropriate to the specific situation.

Step 5: Privacy Breach Notification

Notification helps to ensure Affected Parties can take remedial action, if necessary; and supports a relationship of trust and confidence with the City. The decision to notify Affected Parties will be dependent upon the following considerations:

- Legal obligations;
- Contractual obligations; and
- Any additional risks identified by the City Clerk or designate when completing the Risk Assessment Chart.

If it is determined that the Privacy Breach poses a risk of harm to the Affected Parties, taking into consideration the sensitivity of the Personal Information and whether it is likely to be misused, Affected Parties must be notified as soon as possible. If a law enforcement agency is involved, ensure that notification will not interfere with any active investigations.

Notification should be direct, such as by letter or email correspondence. Indirect notification by public notice must be used only in situations where direct notification is not possible or reasonably practical (e.g. when contact information is unknown or the Privacy Breach affects a large number of individuals).

At minimum, notification to Affected Parties should contain the information described on the Privacy Breach Notification Checklist (Appendix 3), including:

- Details of the extent of the Privacy Breach and the specifics of the Personal Information that was compromised;
- The steps planned to address the Privacy Breach, both immediate and long-term;

- If financial information, or information from government-issued documents were involved, include the following statement in the notification:

  > *"As a precautionary measure, you should monitor and verify all bank accounts, credit card and other financial transaction statements for any suspicious activity. If you suspect misuse of your personal information, you may wish to obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed."*

- An apology to Affected Parties whose Personal Information was breached while in the City's Custody and/or Control;

- Contact information for the City Clerk or designate who would be able to provide additional information and assistance, as requested;

- Directions regarding how to file a formal Privacy Complaint with the I.P.C., should the Affected Party so choose; and,

- The I.P.C. shall be copied on all Privacy Breach Notifications to Affected Parties.

The City Clerk or designate shall determine whether to complete a formal report to the I.P.C., depending on the nature of the Privacy Breach. Privacy Breaches involving the following factors may be reported to the I.P.C.:

- Sensitive Personal Information (e.g. financial, employment, or health information);

- A large number of Affected Parties (e.g. 50 or above);

- Where the Privacy Breach has proven difficult for the City to contain without the assistance of the I.P.C.; or

- In the opinion of the City Clerk in consultation with the Chief Administrative Officer ("C.A.O."), it is determined that it is in the public interest to provide such a report.

Step 6: Mitigate and Prevent

The City Clerk or designate shall take any measures or actions within their authority to mitigate or correct the Privacy Breach as appropriate, having regard to the seriousness of the Privacy Breach and any additional risks identified when completing the Risk Assessment Chart.

Additionally, the City Clerk or designate shall consider if further measures are required to prevent the occurrence of a similar Privacy Breach, and inform appropriate individuals within the City of any findings and/or recommended remedial action(s).

The City Clerk or designate will complete the following steps:

- Review applicable Branch or departmental policies, procedures and practices for the management of Personal Information;

- Review training related to security and privacy, as applicable;

- Ensure individuals are properly trained in any new safeguards related to the Privacy Breach;
- Recommend remedial action(s), as appropriate;
- Develop and implement new security or privacy measures, with the assistance of Information Technology Services;
- Test and evaluate remedial action(s); and
- Advise the I.P.C. of any findings, and work cooperatively with the I.P.C. to make necessary changes, as appropriate.

Step 7: Reporting

Where the Clerk has determined to notify the I.P.C. of a Privacy Breach has been met per Step 5, the City Clerk or designate shall prepare a report to outline the results of the investigation and describe any suggestions to mitigate similar occurrences in the future. If the I.P.C. has been notified, the City Clerk or designate will cooperate with any investigation undertaken in relation to the Privacy Breach.

A report shall be submitted to the appropriate Standing Committee of Council, where:

- The Privacy Breach has affected 50 or above Affected Parties; or,
- In the opinion of the City Clerk in consultation with the C.A.O., it is determined that it is in the public interest to provide such a report.

Suggestions for improvement from the report shall be added to the appropriate Branch or departmental work plan for review and implementation, as appropriate.

Step 8: Logging and Document Retention

The Information Access and Privacy Officer shall maintain a log of all Privacy Incidents and Privacy Breaches, as well as any recommendations resulting from investigations of these incidents and breaches. The log will be used to assist in the provision of reports to the City's Corporate Leadership Team on the number and nature of Privacy Incidents and Privacy Breaches, as appropriate.

All documentation related to identification, containment, investigation, remediation, communication and/or notification of a Privacy Incident or Privacy Breach shall be securely retained by City Clerk Services in accordance with the Records Retention By-law, as applicable.

8.0 I.P.C. Privacy Breach Investigations

When responding to a report or complaint of a Privacy Breach, or initiating their own investigation, the I.P.C. may:

- Assess whether the Privacy Breach has been contained and Affected Parties have been adequately notified;
- Interview any individuals involved in the Privacy Breach;

- Review and provide advice on the City's policies and any other relevant documents;
- Issue a report after the investigation, which may include recommendations; and/or,
- Issue an order to the City.

9.0 Monitoring and Evaluation

City Clerk Services monitors compliance, engagement and awareness of this policy through the following:

- Reviewing results of audits;
- Conducting training and education session evaluations; and
- Conducting Employee surveys.

This Policy is reviewed by the City Clerk or designate at least every three years to ensure its effectiveness and compliance with legislation and current business processes or as required based on legislative changes.

The City Clerk is authorized to make minor or housekeeping amendments to this Policy, as required.

For further information regarding this Policy, please contact City Clerk Services at 905-436-3311 or clerks@oshawa.ca.

10.0 References

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

I.P.C. Privacy Breach Protocol: Guidelines for Government Organizations, Information and Privacy Commissioner of Ontario

Access and Privacy Policy and Procedure

Code of Conduct

Appendix 1 – Privacy Breach Report Form (Page 1)

Oshawa®

Privacy Breach Report Form

This form is to be used by Supervisors and/or Managers to report suspected Privacy Breaches that have occurred in their branch. Consult the City's Privacy Breach Protocol before completing this form. Please complete the form to the best of your abilities, and contact the Information, Access and Privacy Officer if required.

General Information	
Name and Job Title of Supervisor/Manager:	
Date of the breach:	
Branch(es) affected by the breach:	
When and how was the breach discovered?	
Brief description of breach event(s):	

Appendix 1 – Privacy Breach Report Form (Page 2)

Containment	YES	NO
Have the records concerned been retrieved or access to them stopped?	☐	☐
Can you confirm that no copies have been made or retained by the individual(s) who were not authorized to receive the information?	☐	☐
Was the information encrypted, anonymized or otherwise not easily accessible?	☐	☐

Date the system was shut down (if a system was breached):	
Details regarding computer access codes or authorizations revoked or paused:	
Identify and describe any weaknesses in physical or electronic security:	

Provide contact information for unauthorized individual(s) receiving information (if more than one individual attach details on separate sheet)

Name:	Phone Number:	Email Address:

Personal Information	
What personal information was involved?	
Format of records:	
Describe the physical or technical security measures in place at the time of the breach:	

Appendix 1 – Privacy Breach Report Form (Page 3)

Cause and Extent	
Cause of the breach (if known):	
Risk of ongoing or further exposure of the information (e.g. high, medium, low, unknown):	
Type of breach (e.g. isolated incident, accidental exposure, systemic problem, hacking, etc.):	
Number of affected individuals:	
Type of individuals affected (e.g. members of the public, employees, other external parties)	

Report completed by (name, job title):

Date:

Send completed Privacy Breach Report Form to the Information, Access and Privacy Officer in City Clerk Services, copying the appropriate Director and/or Commissioner. **Limit distribution of completed Privacy Breach Report Forms to those individuals who require information about the Privacy Breach as part of their duties and responsibilities.**

Appendix 2 – Privacy Breach Risk Assessment Chart

Privacy Breach Risk Assessment Chart

This chart may be used to assist in determining if a Privacy Breach has occurred that will result in the notification of affected parties. If the answer to all risk factor questions listed below is "no," there is a low probability that personal information has been compromised. The City Clerk, or designate, will determine based on the risk factors below whether the potential privacy breach is a reportable breach according to the Privacy Breach Protocol.

Privacy Breach Risk Factors	YES	NO
Is there a risk of identity theft or other fraud? *Identity theft is a concern if the breach included unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health card numbers, debit card numbers, password information, etc. that can be used for fraud by negative actors.*	☐	☐
Does the loss of information place any individual at risk of physical harm, stalking or harassment?	☐	☐
Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? *This type of harm can occur when a negative actor comes to possess personal information in the custody and/or control of the City related to medical or human resources information (e.g. disciplinary files).*	☐	☐
Could the loss of information result in damage to the reputation of an individual, which may affect business or employment opportunities?	☐	☐
Does the City have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?	☐	☐
Does the breach consist of "sensitive information"? *Including, but not limited to: human resources records (e.g. disciplinary actions, performance reviews), financial information (e.g. credit card numbers, banking information), health information (e.g. diagnosis, WSIB information, workplace accommodations)*	☐	☐

Appendix 3 – Privacy Breach Notification Checklist

Privacy Breach Notification Checklist

This chart may be used to assist in preparing a Privacy Breach Notification to an affected party. The information in the notice should help the individual to reduce or prevent harm that may be caused by the Privacy Breach. Include the information set out below:

Information Requested	Included?
Date of the breach and branch(es) involved	☐
Description of the breach (a general description of what occurred)	☐
Description of the information involved (describe the information inappropriately accessed, collected, used or disclosed)	☐
Steps take to date to control or reduce the harm	☐
Future steps planned to prevent further privacy breaches	☐
Steps the individual can take to mitigate negative impact(s) (provide information about how individuals can protect themselves, e.g. how to contact credit reporting agencies to set up credit watch, information explaining how to change a personal health card number or driver's license number) *If financial information, or information from government-issued documents are involved, include the following in the notice:* *"As a precautionary measure, you should monitor and verify all bank accounts, credit card and other financial transaction statements for any suspicious activity. If you suspect misuse of your personal information, you may wish to obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed."*	☐
Information about how to contact the Information and Privacy Commissioner of Ontario	☐
Organization contact information for further assistance (include contact information for someone within the City who can provide additional information and assistance, and to answer any questions)	☐

Appendix 4 – Privacy Incident and Breach Flow Chart