BRAMPTON

ADMINISTRATIVE DIRECTIVE

Category: Governance

Privacy Protection

Policy Number: GOV-130
Approved by: CAO/CLT – April 1, 2025
Administered by: Information Privacy
Effective Date: April 1, 2025

1. Purpose

The purpose of this Privacy Protection Administrative Directive is to outline the principles and guidelines for ensuring the privacy and confidentiality of personal information collected, used, and disclosed by the City of Brampton in accordance with applicable privacy laws and regulations.

2. Application and Scope

This Privacy Protection Administrative Directive, administered by the Information & Privacy team, applies to City Employees, Elected Officials, Volunteers and Interns, Service Providers and Contractors, Board and Committee Members, and to any other persons providing programs or services on behalf of the City.

The directive applies to any and all handling of personal information within the City, including the Collection, Use, Disclosure, Storage, Protection, Retention, Disposal and Access and Correction.

The directive is pursuant to specific privacy related legislation including all provisions and exemptions therein, such as MFIPPA and PHIPPA.

3. Outcomes

3.1 Formally recognize requirements established by the Provincial and Federal legislation identified below, and to set out the City's approach to compliance.

4. Policy Statements

4.1 There is accountability for privacy.

4.1.1 Privacy protection is everyone's responsibility. MFIPPA provides that accountability for privacy protection rests with the "Head" of an institution. For purposes of the legislation, a municipality is an "institution". Council delegated the powers and duties of the Head to the City Clerk by By-law No.102-90 and Administrative Authority By-Law 216-2017. As Head of the City of Brampton for purposes of MFIPPA, the City Clerk is also the Chief Privacy Officer in the Administrative Authority By-Law 216-2017.

4.1.2 The policy fosters a culture of shared responsibility, where each person contributes to the overall protection of personal data, ensuring that privacy is respected and maintained across the entire organization.

4.2 Training and reference materials are readily available.

4.2.1 Access to training, job aides and reference materials are available to everyone who may handle personal information or personal health information in the course of their duties. This ensures they can quickly

find the information and guidance they need to perform their duties in compliance with privacy laws and policies.

4.3 Policies, procedures and terms of use related to privacy protection are publicly available and easy to access.

4.3.1 Information on the City's privacy protection practices is publicly available in electronic format on our website. A hard (i.e. paper) copy will be provided to any person upon request.

4.3.2 Prior to the collection of personal information, consent for the use and disclosure of the information is obtained.

4.3.3 The City shall obtain consent from affected individuals for particular uses and disclosures of personal information prior to the collection of the information unless legislation permits otherwise. Consent shall be expressed rather than implied where possible, and in writing.

4.3.4 Individuals are made aware of the specific purposes for which their data will be used and who may have access to it. By obtaining consent, the City respects individuals' rights to control their personal information and ensures that data is collected and used in a manner that individuals understand and have agreed to.

4.4 A Notice of Collection is used each time the City collects personal information.

4.4.1 The City provides a notice of collection in advance of the collection of personal information. Notices of collection are provided in written format if possible. Verbal notices of collection are used for service interactions where written notices are impractical, such as telephone interactions involving the City's Contact Centre.

4.4.2 Notices of collection of personal information are clear and transparent and include the following information:

a) The legal authority that permits the collection of the personal information;

b) the purposes for which the personal information is being collected, how it will be used, retained and disclosed; and,

c) the name, title and direct contact information for an individual who can answer questions about the specific collection, use, protection and disposal of personal information.

d) Sample notice of collection:

*Personal information is collected under the authority of the Municipal Act, 2001, S.O. 2001, c. 25. The information will be used or disclosed to **(insert purpose)**, or for a purpose consistent with the Municipal Freedom of Information and Protection of Privacy Act. Questions about the collection of personal information may be directed to the*

following ***(contact name, phone and email) or privacy@brampton.ca.***

4.5 Personal information will not be collected unless necessary.

4.5.1 The City shall not collect more personal information than is required to provide its programs and services. The City is committed to collecting only the personal information that is essential for a specific purpose, avoiding the collection of unnecessary or excessive data.

4.5.2 Personal information will only be used for the purpose for which it was collected.

4.5.3 The City uses and discloses personal information only for the purposes identified in the notice of collection and for which the affected individual has provided consent, except where required by legislation.

4.6 Consent is required to disclose personal information to third parties.

4.6.1 The City will obtain explicit permission from individuals before sharing their personal information with third parties, ensuring that individuals maintain control over who may access their data. Individuals shall be informed about who their information may be shared with and for what purpose. Personal information will only be disclosed to third parties with the express consent of the affected individual, except where required by legislation.

4.6.2 Whenever personal information will be shared with third parties, the City will ensure that an agreement with provisions to protect personal information in accordance with this Administrative Directive and applicable legislation is in place prior to any information being shared.

4.7 Personal Information will not be retained longer than necessary.

4.7.1 Personal information will be retained only for as long as necessary to fulfil the stated purpose as identified in the Records Retention By-Law 272-2014 (amended by By-Law 183-2015), except where required by legislation.

4.7.2 Personal information will be disposed of in compliance with established Records and Information Management policies and procedures and in a secure manner that prevents loss, misuse, theft, or unauthorized access.

4.8 Personal information is protected.

4.8.1 The City will make every reasonable effort to prevent any loss, misuse, disclosure, or modification of personal information.

4.8.2 Appropriate physical and digital security measures will be employed to protect records that contain personal information and to prevent inappropriate use.

4.8.3 Records containing personal information will be appropriately destroyed at the end of the retention period identified in the Records Retention By-Law 272-2014 (amended by By-Law 183-2015), including shredding paper records and permanently deleting electronic records.

4.9 The City will take reasonable steps to ensure the accuracy of personal information in its records.

4.9.1 The City will maintain to the best of its ability, accurate, complete and relevant personal information for the purposes identified in the notice of collection.

4.9.2 The city is committed to maintaining accurate, up-to-date personal information in its records to ensure that the data used for decision-making and service delivery is reliable and correct.

4.9.3 The city will implement procedures to regularly review and update personal information, correcting any inaccuracies as they are identified.

4.10 Individuals have the right to access their personal information and to request correction of their personal information.

4.10.1 Individuals have a right to access their own personal information in a record that is in the custody or under the control of the City, subject to legislated exceptions. Individuals may also request information about the City's use of their personal information and any disclosure of that information to persons outside the City.

4.10.2 To assist the public to identify where personal information may be recorded, the City maintains a Personal Information Bank Register. The Register includes a description of personal information maintained to support each division's programs and activities.

4.11 The City of Brampton does not automatically collect the personal information of persons browsing the City's websites.

4.11.1 Users may browse the City's Website anonymously or register for an online account. Personal information is only collected if it is supplied voluntarily by a user contacting the City via email or an online form, or by setting up an online user account. Most information available on the City's website can be accessed anonymously. A user account is required to access most goods and services online.

4.11.2 The City's web server automatically collects a limited amount of information required to optimize the browsing experience and for statistical reporting. This information includes the user's Internet

Protocol (IP) address, type of browser used, the user's screen size, web pages visited, the date and time of the visit, and the IP address locations to which the user linked while visiting the City's website. To collect this information the City may use cookies, which are temporary files placed on a user's hard drive during a visit to the City's website. None of the collected information is matched or linked to other information that may be available such that an individual user could be identified.

4.11.3 Detailed information on online privacy protection is available in the City's Privacy Statement.

4.12 Privacy Impact Assessments are used to ensure compliance with legislated requirements and established best practices.

4.12.1 A Privacy Impact Assessment (PIA) shall be completed for all new and/or enhanced services, technologies, and/or systems that involve the collection or use of personal information.

4.12.2 PIAs help ensure that the City's handling of personal information complies with relevant privacy laws and regulations. This process allows the City to proactively address privacy concerns, minimizing the likelihood of privacy breaches and enhancing public trust.

4.12.3 Refer to the Privacy Impact Assessment Standard Operating Procedure for complete details.

4.13 Where possible, data sets and information systems should be configured and maintained to facilitate information sharing while protecting personal privacy.

4.13.1 Information is an important corporate asset that supports the delivery of City programs and services. City staff shall share as much information as possible with other City staff, external organizations and the public subject to compliance with MFIPPA, PHIPPA, contracts, non-disclosure agreements and City policies.

4.14 Open Government and Open Data support privacy protection.

4.14.1 The City of Brampton is committed to the principles of open government: greater transparency and accountability, increasing citizen engagement, and driving innovation and economic opportunities through open data, open information, and open dialogue. Data analytics, data matching and data mining activities offer an opportunity to generate economic and social value from City records. However, these activities may only take place if the City can ensure that privacy rights are respected.

4.14.2 Prior to conducting new data analytics, data matching and/or data mining activities, a Privacy Impact Assessment will be conducted and

the City will “de-identify” (in other words, anonymize) the data so that the information is stored and shared such that the identity of affected individuals is not revealed. Further information is available in the City’s Open Data Policy.

4.15 In certain circumstances, legislation requires that individuals be publicly identified.

4.15.1 Participation in certain activities requires that individuals be publicly identified. For example, the Municipal Act, 2001, S.O. 2001, c. 25 requires (with limited and specific exemptions) that the proceedings of Council and Committees, including presentations and submissions by individuals, be open to the public and recorded. Likewise, the Planning Act, R.S.O. 1990, c. P.13 requires that all information related to planning applications, including comments on applications made by individuals, be publicly disclosed. The Lobbyist Registry By-law No. 149-2015 establishes that all individuals engaged in lobbying City officials must be publicly identified.

4.15.2 Whenever an individual will be publicly identified, the City will make this clear prior to the collection of personal information through the use of an appropriate Notice of Collection.

4.16 Privacy complaints are promptly investigated.

4.16.1 Staff members must report all suspected privacy breaches to their supervisor and to the Chief Privacy Officer/City Clerk. Members of the public may report a suspected privacy breach by writing to the Chief Privacy Officer/City Clerk, Office of the City Clerk, 2 Wellington Street West, Brampton, Ontario, L6Y 4R2 or at privacy@brampton.ca or by calling 311.

4.17 Compliance with the Administrative Directive on Privacy Protection is periodically audited.

4.17.1 All internal audits include a mandatory discussion on privacy as part of the audit kick-off meeting.

4.17.2 Information Management staff may periodically review privacy impact assessments and established corporate practices to ensure compliance with the Administrative Directive on Privacy Protection and related procedures and best practices.

5. Roles and Responsibilities

5.1 All employees are required to:

5.1.1 Familiarize themselves with this Administrative Directive;

5.1.2 Comply with this Administrative Directive; and

5.1.3 Report any violation of this Administrative Directive to their supervisor.

5.2 City Clerk

5.2.1 Has overall accountability for privacy protection at the City of Brampton;

5.2.2 Has the powers, duties and responsibilities as the Head under *MFIPPA;*

5.2.3 Is responsible for making privacy-related advice and Privacy Impact Assessments available to business units;

5.2.4 Is responsible for ensuring Personal Information Banks are complete, accurate and up to date; and

5.2.5 Is responsible for administration of this Administrative Directive and for establishing procedures, standards and/or guidelines necessary for its implementation.

5.3 Manager, Access & Privacy

5.3.1 Is responsible for ensuring a Privacy Impact Assessment is completed for all new and/or enhanced services, technologies, and/or systems that involve personal information.

5.3.2 Is responsible for ensuring appropriate notices of collection are in place whenever personal information is collected, and for ensuring that consent has been obtained prior to collection.

5.3.3 Is responsible for approving data sets for inclusion in the open data catalog.

5.3.4 Is responsible for reviewing contracts, as required, to ensure appropriate privacy protections are in place.

5.4 Access and Privacy Coordinator

5.4.1 Develops and delivers privacy-related training.

5.4.2 Coaches and provides privacy-related advice to staff and elected officials.

5.4.3 Conducts Privacy Impact Assessments.

5.4.4 Processes FOI and Routine Disclosure requests.

5.4.5 Makes recommendations to the City Clerk for updates to the Privacy Protection Administrative Directive.

5.4.6 Updates Personal Information Banks.

5.4.7 Initiates the privacy breach protocol and investigates suspected privacy breaches.

5.5 Chief Information Officer

5.5.1 Is responsible for ensuring the security of hardware and software systems containing personal information.

5.5.2 Ensures privacy impact assessments are conducted on all new or modified technologies that involve the collection or use of personal information.

6. Monitoring and Compliance

6.1 Consequences of non-compliance

6.1.1 Failure to follow this Administrative Directive may result in a privacy breach and/or prosecution of a Provincial or Federal offence.

6.1.2 The consequences of a privacy breach may include reputational damage to the City, negative publicity, litigation and financial damages. The City's response to a privacy breach focuses on limiting any damages arising from the breach and on changing systems to prevent future breaches.

6.1.3 City employees acting in good faith and in compliance with this Administrative Directive will not be subject to disciplinary action for privacy breaches; however, failure to adhere to the provisions in this Administrative Directive will result in disciplinary action.

6.1.4 The consequences of conviction of a Provincial or Federal offence may include a fine, reputational damage to the City and reputational damage to affected staff. The legislation provides that staff acting in good faith and to the best of their abilities will not be subject to prosecution. Negligence or willful violation of legislation may result in prosecution of staff and/or the City.

7. Definitions

7.1 Head - the person at the City of Brampton responsible for compliance with *MFIPPA*. The City uses the meaning specified in *MFIPPA*.

7.2 Health Information Custodian - a health care practitioner or health care institution that creates, uses and maintains health care records. The City uses the meaning specified in *PHIPA*.

7.3 Personal Information - any recorded information about an identifiable individual. The City uses the meaning specified in *MFIPPA*.

7.4 Personal Health Information - any recorded information that relates to the physical or mental health of an identifiable individual. The City uses the meaning specified in *PHIPA*.

7.5 Personal Information Bank (PIB) - a collection of records that contain personal information that can be searched and accessed using a person's name, an identifying number or other identifier. The City uses the meaning specified in *MFIPPA*.

7.6 Privacy Breach - inappropriate collection, use or disclosure of personal information.

7.7 Privacy Impact Assessment (PIA) - a formal assessment of privacy obligations, risks and requirements related to a given program, technology, service or personal information bank.

7.8 MFIPPA is the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56

7.9 PHIPA is Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A

7.10 FOI - Freedom of Information

8. References and Resources

This Administrative Directive should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available.

8.1 External references

- *The Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, c. M.56.*
- *Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A*
- *Public Sector and MPP Accountability and Transparency Act, 2014, S.O. 2014, c. 13.*
- *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23)*

8.2 References to related bylaws, Council policies, and administrative directives

- By-law No.102-90
- Administrative Authority By-Law 216-2017
- Records Retention By-Law 272-2014 (amended by By-Law 183-2015)
- Open Data Policy

8.3 References to related corporate-wide procedures, forms, and resources

- Personal Information Bank Register
- Privacy Statement
- Privacy Impact Assessment (PIA)
- Privacy Impact Assessment Standard Operating Procedure

9. Revision History

Date	Description
2014/06/09	Approved by City Clerk on June 9, 2014.
2017/06/09	Next Scheduled Review. (*typically, three years after approval)*
2018/02/14	Approved by CLT on February 14, 2018 - Replaces Personal Information Protection Policy.
2021/02/14	Next Scheduled Review. (*typically, three years after approval)*
2025/04/01	Approved by CAO/CLT on April 1, 2025.
2028/04/01	Next Scheduled Review. (*typically, three years after approval)*