Policy Owner	Corporate Administration, Office of the Regional Clerk, Access and Privacy Office, Deputy Regional Clerk
Approval Body	Council
Approval Date	
Effective Date	
Review by Date	August 2022

1. Policy

Niagara Region shall comply with the Province of Ontario's access to information and privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Access and Privacy Principles
Niagara Region is committed to fostering trust and confidence with the public through its adherence to the following fundamental principles of MFIPPA:

1) Information should be available to the public

Niagara Region shall provide access to information under its custody or under its control, whether through routine disclosure, proactive dissemination, Open Data, and/or through the formal freedom of information request process, in accordance with the principles that:

a. Information should be available to the public; and
b. Necessary exemptions from the right of access should be limited and applied in specific circumstances, such as the protection of personal information, third party information, and confidential government information protected by legal privilege.

2) Individuals shall have access to their own personal information
Niagara Region's divisions, programs, or services which collect, use, retain, disclose, and/or dispose of personal information shall, in consultation with the Access and Privacy Office, develop, implement and annually review procedures for granting individuals' access to their own personal information, including a standard for what information may be provided through routine disclosure and what information may require the individual to submit a freedom of information request.

   Every individual who is given access to his/her personal information is entitled to request correction of the personal information Niagara Region has in its custody or in its control, if the individual believes there is an error or omission.
   - In the event Niagara Region is unable to make a correction due to the inability to verify accuracy, Niagara Region shall instead ensure the request is documented and appended to the information in question reflecting any correction that was requested but not made and the reasons therefore.
   - Additionally, Niagara Region shall ensure that anyone to whom the personal information was disclosed, within the year before the correction was requested, be notified of the correction or the statement of disagreement.

3) Institutions must protect the privacy of individuals with respect to personal information; Niagara Region will:
   a. Establish and maintain a corporate privacy program and procedural framework in accordance with the Canadian Standard Association's (CSA) guiding principles of privacy;
      i. Accountability
      ii. Identifying Collection Purposes
      iii. Consent
      iv. Limiting Collection
      v. Limiting Use, Disclosure & Retention
      vi. Accuracy
      vii. Safeguards
      viii. Openness
      ix. Individual Access
      x. Challenging Compliance

b. Ensure all officials and employees share responsibility for the protection of personal information as further described in the roles and responsibilities identified in this policy;

c. Plan for and ensure that the protection of personal information is embedded in the design of all Niagara Region programs, processes, projects and technology;
   i. Niagara Region's programs and services shall conduct a privacy impact assessment (PIA), in a manner that is proportionate with the privacy risk identified by the PIA screening tool, for any new or modified collection, use, retention, disclosure and/or disposal of personal information, or personal health information.

d. Establish and communicate a set of privacy standards and guidelines to improve the protection of personal information by identifying, investigating, assessing, monitoring, and mitigating privacy risks in Regional programs and services which collect, use, disclose and dispose of personal information;

e. Apply this policy and related policies and practices to the collection, use, retention, disclosure, and disposal of personal information;

f. Clearly communicate to the public how personal information is collected, used, disclosed and disposed;
   i. Niagara Region shall make available for inspection by the public an index of all personal information banks (PIB) in the custody or under the control of the institution. The information should include:
      1. Its name and location;
      2. The legal authority for its establishment;
      3. The types of personal information maintained in it;
      4. How personal information is used on a regular basis;
      5. To whom the personal information is disclosed on a regular basis;
      6. The categories of individuals about whom personal information is maintained; and
      7. The policies and practices applicable to the retention and disposal of the personal information.

ii. Niagara Region will ensure Personal Information Banks receive routine maintenance and updating as required to ensure the accuracy and transparency of the information;

g. Make privacy training mandatory, proportional with their job responsibilities, for all Regional officials and employees with access to personal information to understand their obligations under MFIPPA;

4) Niagara Region shall ensure that reasonable measures, respecting the safeguarding and retention of records in the custody or under the control of Niagara Region, are defined, documented, and administered, taking into account the nature of the records to be protected.

Managing Privacy Incidents and Privacy Breaches

Niagara Region shall work to contain, investigate, and reduce the risk of future incidents when personal information is collected, retained, used, disclosed, or disposed of in ways that do not comply with Ontario's privacy laws.

All privacy incidents shall be immediately reported, or reported as soon as reasonably possible, to Niagara Region's Access and Privacy Office.

2. Purpose

To foster public trust by establishing mandatory requirements and clear responsibilities and accountability for the protection of personal information that is collected, used, disclosed, or disposed of by Niagara Region.

3. Scope

This policy applies to all Niagara Region employees, elected officials, students and volunteers. Niagara Region employees responsible for managing, developing, and entering into contracts with any third party service providers or contractors that involve information that would be subject to this policy are responsible for ensuring that those contractual arrangements are in alignment with this policy.

This policy applies to all personal information including personal health information in the custody or the control of Niagara Region and is not limited by the scope of any individual legislation or regulation with the exception of personal health information in the custody or control of Niagara Region's Health Information Custodians pursuant to PHIPA.

3.1. Roles and Responsibilities

3.1.1. Regional Clerk

a. Provide oversight of and compliance with this Policy and Framework by all Regional Staff.

3.1.2. Corporate Leadership Team

a. Integrate protection of personal information requirements into the development, implementation, evaluation, and reporting activities of divisional programs and services in accordance with this policy and any of its procedures;
b. Promote a culture of business practices that ensure Regional information is shared and accessible to the greatest extent possible, while respecting privacy requirements of personal information and other confidentiality obligations.

3.1.3. Deputy Regional Clerk

a. Develop and implement policies, programs and services for management and protection of personal information based on Privacy by Design principles;
b. Establish privacy standards, guidelines and procedures to support this Policy and Framework;
c. Coordinate the corporate privacy breach protocol and the response to complaints regarding the misuse of personal information;
d. Authorize and sign-off on the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information;

e. Engage the Chief Information Officer to assess the security of any technological system that collects or uses personal information or personal health information.

3.1.4. Freedom of Information Coordinator

a. Accept formal freedom of information (FOI) requests on behalf of Niagara Region and facilitate the search, gathering and redaction of the records, as required;
b. Maintain all records and information pertaining to an FOI request;
c. Review divisional procedures for granting individuals' access to their own personal information, including access through routine disclosure and freedom of information requests;
d. Complete annual reporting to the Information and Privacy Commissioner/Ontario which includes compiling and verifying required data.

3.1.5. Access and Privacy Office

a. Implement this policy, in partnership with Regional Divisions, including the development of required procedures;
b. Review divisional practices for the collection, use, disclosure and disposition of personal information;
c. Consult with business programs to meet privacy requirements as identified in this Policy, applicable legislation, privacy standards and procedures;
d. Investigate reports of privacy breaches and communicate findings to complainant and engage with Legal Services as required;
e. Review and investigate all privacy incidents to determine whether or not a breach has occurred. The Access and Privacy Office will coordinate and manage all privacy breaches according to Niagara Region's Privacy Breach Protocol procedure
f. Conduct Privacy Impact Assessments in consultation with Regional Divisions and programs;
g. Develop, coordinate and deliver privacy training as required by this policy and its associated procedures.

3.1.6. Manager, Information Management Services

a. Oversee, develop and implement corporate strategies, policies, standards, procedures, best practices and programs to promote the Regions records and information management program;

b. Lead records and information training and awareness campaigns;

c. Provide advice and guidance on records and information management policies and related matters.

3.1.7. Chief Information Officer

a. Implement Privacy by Design principles in Enterprise Architecture, information technology policies, standards, procedures and technologies;

b. Conduct Risk Assessments (Threat Risk Assessments, and Vulnerability Assessments) on all technological systems involving the collection or use of personal information prior to implementation or deployment;

c. Execute recommendations identified in Privacy Impact Assessment reports;

d. Provide to the Deputy Regional Clerk the results of all Threat Risk Assessments and Vulnerability Assessments on any technological system that collects or uses personal information or personal health information.

3.1.8. Directors and Divisional Leadership

a. Be accountable for ensuring personal information is collected, used, disclosed and disposed in accordance with legislation and associated regulations, standards and other Regional policies, and in compliance with this policy;

b. Develop, in consultation with the Freedom of Information Coordinator and the Privacy Officer, procedures for granting individuals' access to their own personal information, including a standard for what information may be provided through routine disclosure and what information may require the individual to submit a freedom of information request;

c. Implement this Policy and Framework and communicate to staff under their direction;

d. Restrict access to personal information to those individuals who require access to personal information in order to perform their duties and where access is necessary for the administration of their business;

e. Maintain personal information and develop, and implement processes whereby individuals can view information held about them and what the Region uses it for. These processes will also facilitate individuals needing to correct or update their information;

f. In collaboration with the Privacy Officer, the Chief Information Officer, applicable Commissioner, Procurement staff, and the Chief Administrative Officer, ensure that any contractual arrangements with third party service providers or contractors are in alignment with this policy;

g. Consult with the Deputy Regional Clerk and the Chief Information Officer during the planning stages, before any procurement, and prior to implementation of any technology, system, program or service involving the collection, use, disclosure or disposition of personal information or personal health information.

3.1.9. Niagara Region Personnel

Each individual that collects, uses, discloses, or disposes of information received as part of their duties as a Regional employee including personal information, is accountable for the actions they take with the information including ensuring the information is used only for the purpose it was obtained and is not disclosed to either other employees or non-employees except as permitted in accordance with this policy and applicable legislation whatever form the information is stored or transmitted in. All employees will:

a. Manage personal information that they collect, use, retain, disclose and dispose of for Regional business in accordance with this policy and its procedures to safeguard such information;

b. Take privacy training as required by their role, position, or in consultation with the Access and Privacy Office to ensure the appropriate handling of personal information and to understand their responsibilities to protect privacy in executing their operational duties;

c. Ensure that personal information is only accessible and discussed by authorized users;
d. Report any privacy incidents to the Access and Privacy Office immediately, or as soon as reasonably possible;
e. Be aware of their individual privacy responsibilities as defined by departmental, divisional, or program specific procedures for the collection, use, retention, disclosure, or disposal of personal information;

Each individual should be aware that non-compliance with MFIPPA requirements, risks and consequences may include any or all of the following:

- Loss of trust or confidence in the Niagara Region
- Privacy Breach or breach in confidentiality
- Legal liabilities and proceedings
- Investigation by privacy oversight bodies (IPC)
- IPC Orders issued against Niagara Region, its policies and/or employee practices
- Negative media coverage for Niagara Region, Regional departments services and programs

Under MFIPPA s.42(2), any individual who willfully acts in contravention of MFIPPA, requests information under false pretenses, obstructs an investigation by the IPC or fails to follow an order by the IPC is liable to a fine of up to $5,000.

Definitions

MFIPPA means the *Municipal Freedom of Information and Protection of Privacy Act* (Ontario) and its regulations, as amended from time to time.

Personal Information means all recorded information that is about an identifiable individual or is defined or deemed to be “personal information” pursuant to any laws or regulations related to privacy or data protection that are applicable to the Regional Municipality of Niagara (including, without limitation, any information that constitutes “personal information” as such term is defined by MFIPPA or “personal health information” as such term is defined by PHIPA).

Privacy Breach means any inappropriate or unauthorized collection, use, retention, disclosure, or disposal of personal information.

Privacy by Design means the consideration of privacy during the design process that integrates the protection of "personal information" directly into the technology/system through creation, operation, and management of the system or technology itself.

Privacy Impact Assessment (PIA) means the tool used by the corporation to review any change to the collection, use, retention, disclosure, or disposal of "personal information" to assess the risks to privacy associated with the change, and to provide recommendations on how to mitigate these risks.

Privacy Incident means and inappropriate or unauthorized action that involves data, information or records which include "personal information" that may lead to the discovery of a "privacy breach".

Threat Risk Assessment (TRA) means the tool use by the corporation to identify, analyzing and reporting the risks associated with an information technology system's potential vulnerabilities and threats.

Vulnerability Assessment (VA) means the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the corporation with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately

4. References and Related Documents.

4.1. Legislation, By-Laws and/or Directives

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);

Niagara Region Retention By-law

Delegation of Head by-law

4.2. Procedures

Privacy breach protocol

5. Related Policies

Personal Health and Information Protection Act (PHIPA) Policy

6. Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

Approver(s)	Approved Date	Effective Date

Revision History

Revision No.	Date	Summary of Change(s)	Changed by