THE MUNICIPAL CORPORATION OF THE TOWNSHIP OF ARMOUR
BY-LAW NUMBER 69-2026

BEING A BY-LAW TO ADOPT A COMPREHENSIVE PRIVACY MANAGEMENT PROGRAM FOR THE TOWNSHIP OF ARMOUR.

WHEREAS Section 8 of the *Municipal Act, 2001*, S.O. 2001, c. 25, provides that a municipality has the capacity, rights, powers, and privileges of a natural person for the purpose of exercising its authority under this or any other Act;

AND WHEREAS Section 227 of the Municipal Act, 2001 outlines municipal officers' and employees' responsibility to implement Council decisions and related administrative procedures;

AND WHEREAS the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), R.S.O. 1990, c. M.56, mandates the protection of personal privacy and establishes strict statutory guidelines for the collection, retention, security, and disposal of personal information in the custody or control of local authorities;

AND WHEREAS recent amendments to provincial legislation mandate that municipal institutions implement formalized Privacy Management Programs, Privacy Impact Assessments, and Breach Protocols;

AND WHEREAS the Council of the Township of Armour deems it necessary and expedient to adopt an integrated suite of corporate privacy, vendor risk, and artificial intelligence governance policies to ensure accountability, transparency, cybersecurity readiness, and public trust;

NOW THEREFORE the Council of the Municipal Corporation of the Township of Armour enacts as follows:

1. **ADOPTION OF CORE POLICIES**

That the following policies, attached hereto as Schedules "A" through "G" and forming an integral part of this By-law, are hereby approved and adopted:

- **Schedule "A":** Privacy Management Program Policy
- **Schedule "B":** Privacy Impact Assessment (PIA) and Privacy Protection Policy
- **Schedule "C":** Freedom of Information and Access to Records Policy
- **Schedule "D":** Privacy Breach Response Policy
- **Schedule "E":** Artificial Intelligence and Emerging Technology Policy
- **Schedule "F":** Vendor Privacy and Security Standard Policy
- **Schedule “G”:** Information Asset Register Policy

2. **ADMINISTRATION AND DELEGATION**

That the Clerk is designated as the operational Head and Privacy Officer under MFIPPA and is authorized to maintain the Information Asset Register, establish procedural guides, and execute statutory tasks defined within these schedules. The Chief Administrative Officer retains structural oversight for technical vendor selections and final corporate system approvals.

3. **SEVERABILITY**

If any provision of this By-law is declared invalid, the remaining provisions shall remain in full force and effect.

4. **REPEAL OF CONFLICTING POLICIES**

That any conflicting previous policies, resolutions, or by-law provisions are hereby repealed or amended accordingly.

5. **EFFECTIVE DATE**

That this By-law shall come into force and take effect on January 1, 2027.

Read in its entirety, approved, signed and the seal of the Corporation affixed thereto and finally passed in open Council this 10th day of November, 2026.

Original signed by Rod Ward
Rod Ward, Mayor

Original signed by Charlene Watt
Charlene Watt, Municipal Clerk

Privacy Management Program Policy

1. PURPOSE

The Township of Armour ("the Township") is committed to protecting the privacy of individuals and ensuring the responsible management of personal information in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and other applicable legislation.

The purpose of this Policy is to establish the Township's Privacy Management Program, providing a governance framework for the lawful collection, use, disclosure, retention, protection, and disposal of personal information. The Policy promotes accountability, transparency, and continuous improvement while supporting the responsible use of technology, including cloud services and artificial intelligence.

2. SCOPE

This Policy applies to:

- Council members;
- all employees, volunteers, contractors, consultants, and agents acting on behalf of the Township;
- all Township departments, boards, committees, and other bodies operating under the authority or direction of the Township, where applicable;
- all records and information systems, regardless of format, including paper records, electronic records, cloud services, digital applications, and artificial intelligence tools used to deliver municipal programs and services.

3. DEFINITIONS

For the purposes of this Policy:

"Artificial Intelligence (AI)" means a machine-based system that uses data and computational methods to infer how to generate predictions, content, recommendations, decisions, or other outputs that can influence physical or digital environments. AI systems may operate with varying degrees of autonomy and may adapt after deployment. For the purposes of this Privacy Management Program, AI includes systems used to collect, analyze, infer, generate, or otherwise process personal information, including machine learning, generative AI, and AI-supported automated decision-making tools.

"Breach (Privacy Breach)" means an incident involving unauthorized collection, access, use, disclosure, retention, disposal, loss, or compromise of personal information.

"Custody or Control" means records that are in the possession of the Township or for which the Township has authority or responsibility to manage.

"Head" means the individual designated as the Head of the institution under MFIPPA.

"Information Asset Register (IAR)" means the Township's administrative inventory of information assets, including records, systems, databases, applications, and business processes that involve the collection, use, disclosure, retention, or disposal of information, including personal information, maintained to support privacy management, records management, information security, and legislative compliance. The Information Asset Register is maintained as an internal governance and administrative tool to support privacy management, records management, information security, and legislative compliance. The Township may also maintain or publish an inventory of personal information holdings where appropriate to support transparency and accountability.

"Personal Information" means recorded information about an identifiable individual as defined by applicable privacy legislation.

"Privacy by Design" means an approach that incorporates privacy protection into the design, planning, implementation, operation, and disposal of programs, services, technologies, and business processes.

"Privacy Impact Assessment (PIA)" means a documented process used to identify, evaluate, and mitigate privacy risks associated with new or substantially changed initiatives involving personal information.

"Privacy Management Program (PMP)" means the Township's framework of governance, policies, procedures, training, monitoring, and accountability measures established to protect personal information and support compliance with privacy obligations.

"Privacy Risk" means the potential for an individual's privacy to be adversely affected through the collection, use, disclosure, retention, loss, unauthorized access, or other handling of personal information.

"Real Risk of Significant Harm (RROSH)" means the statutory threshold used to determine whether a privacy breach must be reported to the Information and Privacy Commissioner of Ontario and affected individuals must be notified, as required by MFIPPA and applicable regulations. The assessment considers whether it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to an individual. The nature and sensitivity of the personal information, the circumstances of the incident, and the likelihood and potential consequences of misuse shall be considered in accordance with applicable legislation and guidance.

"Records" means recorded information in any format, including paper and electronic records, created, received, or maintained by or on behalf of the Township.

"Records Access and Privacy Designate" means a Township employee designated by the Clerk to assist with the administration and operational responsibilities associated with records access, privacy protection, and implementation of the Township's Privacy Management Program. The designation does not establish a separate statutory office or transfer the statutory responsibilities of the Head under MFIPPA.

"Significant Harm" means harm that includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record, and damage to or loss of property, as applicable under MFIPPA and its regulations.

"Third-Party Service Provider" means an external organization or individual engaged by the Township to provide services involving access to or handling of Township information or personal information.

4. LEGISLATIVE AUTHORITY

This Policy is established pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and shall be administered in accordance with applicable legislation, regulations, municipal policies, records retention requirements, and guidance issued by the Information and Privacy Commissioner of Ontario.

Where legislation imposes more stringent privacy requirements, those requirements shall prevail.

5. PRIVACY MANAGEMENT PRINCIPLES

The Township shall manage personal information in accordance with the following principles:

Accountability

The Township is responsible for personal information under its custody or control and shall establish appropriate policies, procedures, and safeguards to protect that information.

Transparency

The Township shall provide clear information regarding the collection, use, disclosure, and protection of personal information.

Lawful Collection and Use

Personal information shall only be collected, used, or disclosed where authorized by law and required for a legitimate municipal purpose.

Data Minimization

The Township shall collect, use, and retain only the minimum personal information necessary to fulfill an authorized purpose.

Security

Appropriate administrative, technical, and physical safeguards shall protect personal information from unauthorized access, use, disclosure, loss, or destruction.

Privacy by Design

Privacy considerations shall be incorporated into municipal programs, services, technologies, and business processes from planning through disposal.

Retention and Secure Disposal

Personal information shall be retained in accordance with applicable legislation, the Township's records retention and disposition requirements, archival obligations, legal holds, and other legal requirements. Information shall not be retained indefinitely without an authorized purpose. When eligible for disposition, it shall be securely destroyed, erased, or transferred in accordance with approved procedures.

Continuous Improvement

The Township shall regularly review and improve privacy practices in response to legislative, technological, and operational changes.

6. PRIVACY GOVERNANCE STRUCTURE

Council approves this Policy and significant amendments, provides oversight of privacy governance and significant privacy risks, and ensures appropriate resources are available to support privacy obligations.

The Clerk, as the Head under MFIPPA and Privacy Officer, administers the Township's privacy responsibilities, oversees privacy compliance, manages privacy complaints and breach response, supports Privacy Impact Assessments, maintains privacy governance documentation, and acts as the Township's liaison with the Information and Privacy Commissioner of Ontario.

The Chief Administrative Officer supports the implementation of this Policy, promotes privacy governance and responsible information management practices, and assists with operational privacy requirements, vendor reviews, and organizational compliance.

Departments, employees, volunteers, and contractors acting on behalf of the Township comply with this Policy and related procedures, protect personal information in their care, use

information only for authorized purposes, report suspected privacy breaches, complete required training, and cooperate with privacy reviews and investigations.

Records Access and Privacy Support may be designated by the Clerk to one or more Township employees to assist with the administration and operational implementation of the Township's Privacy Management Program and related records access and privacy responsibilities. Such designated employees may be assigned duties relating to the coordination and processing of Freedom of Information (FOI) requests, records searches, privacy impact assessment coordination, maintenance of the Information Asset Register, privacy training and awareness, privacy breach documentation, records management, privacy compliance monitoring, and other administrative or operational requirements established under this Policy and its supporting schedules. The Clerk shall determine the scope of delegated duties and provide appropriate direction and oversight. The designation of duties does not establish a separate statutory office or transfer the Clerk's responsibilities as Head under MFIPPA or as the Township's Privacy Officer. All statutory decisions, determinations, approvals, and responsibilities assigned to the Head or Clerk under applicable legislation shall remain with the Clerk unless otherwise authorized by law.

7. PRIVACY MANAGEMENT PROGRAM REQUIREMENTS

The Township shall maintain a coordinated Privacy Management Program consisting of this Policy and the supporting policies adopted under the applicable By-law.

The Program shall include the following components.

Privacy Impact Assessment and Privacy Protection

The Township shall maintain a process for identifying, assessing, documenting, and mitigating privacy risks associated with municipal programs, services, technologies, information-sharing arrangements, and other initiatives involving personal information.

The detailed requirements for PIA screening, full assessments, privacy notices, risk mitigation, and review shall be established in Schedule “B” — Privacy Impact Assessment (PIA) and Privacy Protection Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

Departments shall consult the Clerk or designate and complete required screening before implementing or materially changing initiatives that may affect personal information, wherever practicable.

Freedom of Information and Access to Records

The Township shall maintain procedures for receiving, processing, and responding to requests for access to records and correction of personal information under MFIPPA.

The procedures shall support statutory access rights, lawful exemptions, appropriate protection of third-party information, consistent decision-making, and compliance with applicable response deadlines and fee requirements.

Detailed operational requirements shall be established in Schedule "C" — Freedom of Information and Access to Records Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

Privacy Breach Response and RROSH Assessment

The Township shall maintain a documented process for reporting, containing, investigating, assessing, documenting, and responding to actual or suspected privacy breaches involving personal information under its custody or control.

Every suspected privacy breach shall be promptly reported to the Clerk or designate and assessed to determine the nature and scope of the incident, the personal information affected, the individuals potentially impacted, and the appropriate containment and mitigation measures.

The Township shall conduct and document a Real Risk of Significant Harm (RROSH) assessment where required by applicable legislation and, as a matter of privacy governance, for suspected breaches involving personal information.

The RROSH assessment shall consider, at a minimum:

- The sensitivity and nature of the personal information involved.
- The circumstances of the breach, including the extent of unauthorized access, use, disclosure, loss, or theft.
- The probability that the personal information has been, is being, or will be misused.
- The number of individuals affected and the potential consequences for those individuals.
- The availability of measures that affected individuals can take to reduce the likelihood of harm or mitigate its effects.
- Relevant IPC guidance and any additional factors prescribed by applicable legislation.

The assessment shall determine whether the applicable statutory RROSH threshold is met. The assessment and its rationale shall be documented, including the information considered, the determination reached, any uncertainties, the decision-maker, and the measures taken or proposed to address the incident.

Where the applicable statutory threshold is met, the Township shall report the breach to the IPC and notify affected individuals as soon as feasible, in accordance with MFIPPA and applicable regulations, unless notification is prohibited by law. Any other prescribed reporting or notification circumstances shall also be addressed.

Where the statutory threshold is not met, the Township shall document the determination and rationale and implement any appropriate corrective or preventive measures. A determination that the threshold is not met shall not prevent the Township from notifying affected individuals or taking other action where required or appropriate under applicable law and guidance.

The Township shall maintain records of breaches and associated assessments, reports, notifications, and corrective actions in accordance with applicable legislative and records management requirements.

The Township shall comply with the privacy breach reporting, individual notification, recordkeeping, and annual reporting requirements imposed by MFIPPA and its regulations, including requirements that come into force on January 1, 2027. Where reporting or notification is required, the Township shall act as soon as feasible after the required determination and in the prescribed form and manner. The Clerk or designate shall coordinate the retention of required breach records and the preparation and submission of applicable annual reports to the IPC.

Detailed responsibilities, assessment procedures, notification requirements, documentation standards, and corrective actions shall be established in Schedule “D” — Privacy Breach Response Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

Artificial Intelligence and Emerging Technology

The Township shall ensure that the use of AI and emerging technologies involving personal information is assessed and managed in accordance with applicable law and Township privacy and security requirements.

Privacy considerations shall be addressed before adopting or materially changing technology that may affect the collection, use, disclosure, security, retention, or accuracy of personal information.

Detailed requirements shall be established in Schedule “E” — Artificial Intelligence and Emerging Technology Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

Vendor Privacy and Security

The Township shall assess and manage privacy and information security risks associated with third-party service providers that access, store, process, or otherwise handle Township information.

Contracts and service arrangements shall include appropriate privacy, confidentiality, security, breach reporting, retention, deletion, and cooperation obligations, as applicable.

Detailed requirements shall be established in Schedule “F” — Vendor Privacy and Security Standard Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

Information Asset Register

The Township shall maintain an Information Asset Register to support the identification and management of information assets and activities involving personal information.

The Register shall support privacy impact assessments, records management, information security, vendor oversight, breach response, and legislative compliance.

The Clerk or designate shall coordinate the maintenance and periodic review of the Register in accordance with Schedule “G” — Information Asset Register Policy in the Comprehensive Privacy Management Program By-law for the Township of Armour.

The Information Asset Register is an internal governance tool and does not replace any statutory Personal Information Bank index, public register, or other disclosure requirement that may apply.

Notice of Collection

The Township shall provide a Notice of Collection when required by MFIPPA or other applicable legislation.

The Notice of Collection shall identify:

- The legal authority for the collection.
- The principal purposes for which the personal information is collected.
- The title and business contact information of a Township official who can answer questions about the collection.

The notice shall be provided at the time of collection, where practicable, and shall be clear, accessible, and appropriate to the relevant municipal program or service.

Departments are responsible for ensuring that notices used in their programs and services accurately describe the collection and intended use of personal information. The Clerk or designate shall provide guidance and review notices where appropriate.

The standard Notice of Collection template is provided in Appendix A to this Policy. The template shall be customized for the relevant collection activity and shall not be used without confirming the applicable legal authority and purpose.

Detailed privacy protection requirements, including PIA screening and assessment procedures, are established in Schedule “B” — Privacy Impact Assessment (PIA) and Privacy Protection Policy.

Records Management and Information Security

The Township shall manage records containing personal information in accordance with applicable legislation, approved retention schedules, and records management requirements.

Administrative, technical, and physical safeguards shall be maintained to protect personal information throughout its lifecycle.

The detailed requirements established under the supporting policies shall operate together with the Township’s applicable records management, information security, procurement, and administrative policies.

8. TRAINING AND AWARENESS

The Township shall provide privacy training to employees and other individuals who collect, access, use, disclose, or manage personal information.

Training shall include, as appropriate:

- MFIPPA obligations, including privacy protection and access to information requirements;
- collection, use, disclosure, and retention requirements for personal information;
- Privacy Impact Assessment (PIA) requirements and privacy risk assessment practices;
- privacy breach identification, reporting, response, and mitigation procedures, including RROSH assessments and mandatory breach notification protocols;
- secure handling and protection of personal information;
- records management responsibilities, including knowledge of the Township’s Routine Disclosure and Active Dissemination of Municipal Records Policy;
- information security practices;
- Vendor Privacy and Security Standard requirements for managing third-party access to Township information; and
- appropriate use of digital technologies, including artificial intelligence tools and emerging technologies.

Training shall be provided upon commencement of employment or engagement, periodically thereafter, and when significant changes occur.

9. MONITORING, REPORTING AND CONTINUOUS IMPROVEMENT

The Township shall monitor compliance with this Policy through appropriate reviews, audits, Privacy Impact Assessments, breach investigations, and other governance activities.

The Clerk or designate may assist in preparing periodic privacy and access to information reports under the direction of the Clerk for Council, including where appropriate:

- access request volumes and processing performance (tracked in business days);
- privacy breaches, associated RROSH determinations and corrective actions;
- Privacy Impact Assessments completed;
- training completion;
- periodic review and maintenance of the Township's Personal Information Inventory (Information Asset Register);
- significant privacy risks; and
- recommendations for improvement.

The Township shall update the Privacy Management Program in response to:

- legislative changes;
- Information and Privacy Commissioner guidance;
- audit findings;
- privacy incidents;
- technological developments; and
- operational improvements.

10. RELATED POLICIES AND DOCUMENTS

This Policy shall be read together with the following policies adopted by Council and attached to the applicable Township By-law:

Schedule “B”: Privacy Impact Assessment (PIA) and Privacy Protection Policy.

Schedule “C”: Freedom of Information and Access to Records Policy.

Schedule “D”: Privacy Breach Response Policy.

Schedule “E”: Artificial Intelligence and Emerging Technology Policy.

Schedule “F”: Vendor Privacy and Security Standard Policy.

Schedule “G”: Information Asset Register Policy.

By-law #46-2023: Freedom of Information & Routine Disclosure Policy (Policy ADM-007)

The Notice of Collection template attached as Appendix A forms part of this Policy.

11. REVIEW

This Policy shall be reviewed by the Clerk at least once during each term of Council or sooner where legislative, technological, or operational changes require review.

12. EFFECTIVE DATE

This policy comes into effect on the date approved by Council.

APPENDIX A

NOTICE OF COLLECTION TEMPLATE

Township of Armour — Notice of Collection

Personal information is collected under the authority of

[identify the applicable statute, regulation, or by-law and relevant provision].

The information will be used for [identify the principal purposes for which the information is collected and used].

Questions about the collection or use of this personal information may be directed to:

[Name or position title]
Township of Armour
P.O. Box 533, 56 Ontario Street
Burk's Falls, Ontario P0A 1C0
705-382-3332
[Business email address]

Departmental Privacy Inventory: Illustrative Collection Activities

The following table identifies examples of municipal activities that may involve personal information. It is intended to support privacy awareness, departmental reviews, and maintenance of the Township's Information Asset Register. It is not an exhaustive inventory of all information holdings, does not independently authorize the collection or use of personal information, and does not replace a collection-specific Notice of Collection where one is required.

Departments shall confirm the applicable legal authority, purposes of collection, information collected, and any applicable notice requirements for each program or activity.

Department or Functional Area	Municipal Activities and Examples of Personal Information Collection	Illustrative Municipal Authority / Legislation	The Information Will Be Used For
Clerk's Department / Legislative Services	Freedom of information requests; access and correction requests; public inquiries and correspondence; delegation requests; Council and committee submissions; meeting registrations; complaints; records management; municipal archives; privacy complaints; public consultations.	*Municipal Freedom of Information and Protection of Privacy Act*; *Municipal Act, 2001*.	Administering access and correction requests, responding to inquiries and complaints, coordinating Council and committee business, managing municipal records and archives, addressing privacy matters, and administering public consultation processes.
Finance and Treasury	Property taxation and billing inquiries; payment arrangements; accounts payable and receivable; vendor payments; reimbursement claims; financial assistance applications; identifiable financial information.	*Municipal Act, 2001*; *Assessment Act*.	Administering property taxation, billing, payments, accounts, reimbursements, financial assistance programs, financial reporting, and related municipal financial administration.
Building and Planning	Building permit applications; planning applications; zoning and development inquiries;	*Building Code Act, 1992*; *Planning Act*.	Processing permit and planning applications, reviewing development proposals, conducting

	consent and minor variance applications; site plan submissions; inspection records; correspondence from property owners and applicants.		inspections, administering applicable building and planning requirements, and communicating with applicants and property owners.
Public Works / Roads and Infrastructure	Road maintenance requests; drainage and culvert concerns; road occupancy and entrance permits; damage claims; infrastructure service requests; public works complaints.	*Municipal Act, 2001*; *Public Transportation and Highway Improvement Act*.	Administering road and infrastructure services, processing permits and service requests, investigating complaints and damage claims, coordinating maintenance, and communicating with affected residents and property owners.
Fire Services and Emergency Management	Emergency response records; incident reports; fire inspection records; fire prevention programs; emergency planning and assistance records; emergency calls.	*Fire Protection and Prevention Act, 1997*; *Emergency Management and Civil Protection Act*.	Delivering fire protection and prevention services, responding to emergencies, documenting incidents, conducting inspections, coordinating emergency planning, and administering authorized emergency management activities.
By-law Enforcement	By-law complaints; investigation records; witness statements; enforcement correspondence; inspection records; notices of violation; alleged violations.	*Municipal Act, 2001*; *Building Code Act, 1992*; *Planning Act*.	Receiving and investigating complaints, conducting inspections, administering and enforcing applicable by-laws, documenting investigations, issuing notices, and managing enforcement proceedings.
Animal Control and Licensing	Dog licensing; animal-related complaints; animal incident reports; licence	*Municipal Act, 2001*; *Dog Owners' Liability Act*.	Administering animal licensing and control services, responding to animal-related complaints

	applications; animal ownership information.		and incidents, maintaining licensing records, and enforcing applicable requirements.
Recreation, Parks and Facilities	Recreation registrations; participant and parent or guardian contact details; facility rental applications; park and pavilion bookings; event permits; program evaluations.	*Municipal Act, 2001*.	Registering participants, administering recreation programs and facility rentals, coordinating bookings and events, communicating with participants and guardians, and evaluating municipal recreation services.
Human Resources / Corporate Administration	Employment applications; recruitment records; employee files; attendance; workplace accommodation requests; workplace investigations; training; health and safety incidents.	*Municipal Act, 2001*; *Employment Standards Act, 2000*; *Occupational Health and Safety Act*.	Administering recruitment, employment, payroll-related processes, attendance, workplace accommodation, employee training, workplace investigations, and occupational health and safety obligations.
Procurement and Contract Administration	Requests for proposals and quotations; supplier and contractor records; sole proprietor information; conflict-of-interest declarations; procurement submissions.	*Municipal Act, 2001*.	Administering procurement processes, evaluating submissions, verifying supplier and contractor information, managing contracts, assessing conflicts of interest, and maintaining procurement and financial accountability records.
Legal Services / Risk Management / Insurance	Claims against the Township; incident reports; insurance documentation; legal correspondence; litigation records; supporting documents containing personal information.	*Municipal Act, 2001*; *Limitations Act, 2002*.	Assessing and managing claims, administering insurance matters, obtaining legal advice, managing disputes and litigation, documenting incidents, and protecting

			the Township's legal and financial interests.
Information Technology / Information Security	User account administration; access logs; security monitoring; system audit trails; device management; access permissions.	*Municipal Freedom of Information and Protection of Privacy Act*.	Administering user accounts and permissions, maintaining municipal information systems, monitoring system security, investigating security incidents, maintaining audit trails, and protecting the confidentiality, integrity and availability of information.
Corporate Security / Municipal Facilities	Video surveillance; building access control; visitor records; facility security incidents; security investigations involving identifiable individuals.	*Municipal Act, 2001*; *Municipal Freedom of Information and Protection of Privacy Act*.	Protecting municipal facilities, managing authorized access, maintaining building security, investigating security incidents, and supporting the safety of employees, visitors and municipal property.
Elections Administration	Municipal election administration; candidate and voter-related records maintained by the Township; election worker applications; election inquiries.	*Municipal Elections Act, 1996*.	Administering municipal elections, processing election-related applications and inquiries, coordinating election workers, maintaining required election records, and fulfilling statutory election responsibilities.
Community Services / Grants and Programs	Community grant applications; funding requests; program registrations; applications for municipal assistance; personal or financial supporting documents.	*Municipal Act, 2001*.	Assessing eligibility for municipal grants and assistance, administering approved programs, processing applications, verifying supporting information, communicating with applicants, and monitoring

			program delivery and accountability.
Communications / Public Engagement	Public consultation registrations; identifiable survey responses; mailing lists; newsletter subscriptions; public inquiries; event registrations; website submissions.	*Municipal Act, 2001*; *Municipal Freedom of Information and Protection of Privacy Act*.	Administering public engagement and consultation activities, responding to inquiries, distributing requested municipal communications, coordinating events, and analyzing feedback to inform municipal programs and services.
Information Management / Archives	Records access requests; archival research inquiries; historical records services; requests involving personal information; municipal archival records.	*Municipal Freedom of Information and Protection of Privacy Act*; *Municipal Act, 2001*.	Managing and preserving municipal records, responding to access requests, facilitating authorized archival research, applying retention and disposition requirements, and supporting records retrieval and accountability.
Digital Services / Cloud Applications / Artificial Intelligence	Online applications and forms; cloud-based service delivery; digital identity or account registration; third-party platforms; AI-enabled tools processing personal information.	*Municipal Freedom of Information and Protection of Privacy Act*; legislation authorizing the applicable municipal program.	Delivering and administering online municipal services, managing user accounts, processing applications, supporting authorized digital workflows, improving service delivery, and using approved technology tools for authorized municipal purposes.

Privacy Impact Assessment and Privacy Protection Policy

1. PURPOSE

The Township of Armour recognizes that privacy protection is fundamental to maintaining public trust and confidence in municipal government.

The purpose of this Policy is to establish a comprehensive framework governing the assessment, management and protection of personal information throughout the lifecycle of municipal programs, services, technologies and business processes.

This Policy establishes mandatory requirements for conducting Privacy Impact Assessments (PIAs) before implementing or substantially modifying initiatives involving personal information.

The Township adopts a proactive Privacy by Design approach whereby privacy protection is incorporated into planning, procurement, implementation, operation, maintenance and disposal rather than being addressed only after implementation.

2. SCOPE

This Policy applies to all Township of Armour employees, officers, contractors, consultants, volunteers, and any other individuals acting on behalf of the Township who plan to implement a new initiative or make a significant change to an existing program, service, system, technology, or business process involving personal information. The Policy applies regardless of whether information exists electronically, on paper, in audio recordings, photographs, video, GIS, cloud systems, portable devices or backup media.

3. DEFINITIONS

For the purposes of this Policy:

“Personal Information” means recorded information about an identifiable individual as defined by applicable privacy legislation.

“Privacy Impact Assessment (PIA)” means a documented process used to identify, evaluate, and mitigate privacy risks associated with new or substantially changed initiatives involving personal information.

“Privacy by Design” means an approach that incorporates privacy protection into the design, planning, implementation, operation, and disposal of programs, services, technologies, and business processes.

"Records Access and Privacy Designate" means a Township employee designated by the Clerk to assist with the administration and operational responsibilities associated with records

access, privacy protection, and implementation of the Township's Privacy Management Program. The designation does not establish a separate statutory office or transfer the statutory responsibilities of the Head under MFIPPA.

4. LEGISLATIVE AUTHORITY

This Policy is adopted pursuant to and shall be interpreted consistently with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the Municipal Act, 2001, the Archives and Recordkeeping Act, 2006, where applicable, the Electronic Commerce Act, 2000, where applicable, the Ontario Human Rights Code, where applicable, the Occupational Health and Safety Act where employee personal information is involved, applicable regulations issued under MFIPPA, Information and Privacy Commissioner of Ontario (IPC) guidance on Privacy Impact Assessments and the Privacy by Design Framework, and applicable municipal governance, records retention, information management, and privacy requirements.

Where another Act imposes more stringent privacy requirements, those requirements prevail.

5. RESPONSIBILITIES

Council approves this Policy and ensures appropriate resources are available to support privacy obligations.

The Clerk oversees the implementation and compliance with this Policy; determines whether a technology, system, program, or service requires a Privacy Impact Assessment (PIA); supports PIA completion; provides guidance on privacy risks; and develops, maintains, and provides PIA tools and resources.

Department Heads consult with the Clerk to determine PIA requirements; consult with the Chief Administrative Officer and Information Technology where technology is involved; collaborate with other departments on initiatives with privacy implications; ensure resources are available for privacy risk management activities; complete PIA reports and accept identified departmental privacy risks; ensure the protection of personal information and personal health information handled by their department or contracted third parties and subcontractors; ensure staff comply with PIA requirements; and manage identified privacy risks in accordance with applicable project management practices.

The Chief Administrative Officer supports Department Heads with technological and security considerations related to PIAs; promotes awareness and implementation of this Policy; ensures PIA guidance, resources, and training materials are available to staff; and assists with PIA completion. The Chief Administrative Officer must provide final approval of all PIAs.

6. GUIDING PRINCIPLES

The Township shall manage personal information according to the following principles.

6.1 Accountability

The Township remains accountable for all personal information under its custody or control regardless of whether information processing is undertaken internally or by third-party service providers.

6.2 Privacy by Design

Privacy protection shall be embedded into every municipal process from conception through disposal.

6.3 Necessity

Only personal information demonstrably necessary for municipal purposes shall be collected.

6.4 Proportionality

Privacy risks shall be proportionate to operational need.

6.5 Transparency

Residents shall understand why personal information is collected, how it is used, and when it may be disclosed.

6.6 Security

Personal information shall be protected through administrative, physical and technical safeguards appropriate to its sensitivity.

6.7 Continuous Improvement

Privacy controls shall evolve as technology, legislation and municipal operations change.

7. PRIVACY BY DESIGN

The Township adopts the following seven Privacy by Design principles Privacy shall be considered during planning, procurement, implementation, operation, retention and disposal.

Every project shall incorporate:

1. Proactive not reactive
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality

5. End-to-end lifecycle protection
6. Visibility and transparency
7. Respect for user privacy

These principles shall be considered throughout the lifecycle of an initiative, including project initiation, budgeting, procurement, contract development prior to implementation, implementation, operational review, and system retirement through appropriate retention and disposition practices.

8. PRIVACY IMPACT ASSESSMENT (PIA) FRAMEWORK

8.1 General

A Privacy Impact Assessment (PIA) is the Township's primary privacy risk management tool. It is designed to identify, evaluate, and mitigate privacy risks before they affect individuals or municipal operations.

When a PIA is deemed to be necessary for a project, it is to be completed at the earliest opportunity available.

Every PIA shall:

- identify applicable legislative requirements;
- document the purpose and authority for collecting personal information;
- evaluate privacy risks;
- recommend mitigation measures;
- assign responsibility for implementing mitigation strategies;
- document residual risks accepted by the Township; and
- become part of the official municipal record.

Completion of a PIA shall occur **before procurement, implementation, or deployment** whenever practical.

8.2 Objectives of a PIA

The objectives of every Privacy Impact Assessment are to ensure compliance with MFIPPA and other applicable legislation; protect the privacy rights of individuals; support transparency and accountability; identify unnecessary collection, use, or retention of personal information; identify operational and cybersecurity risks; reduce the likelihood of privacy breaches; improve public confidence; support sound procurement decisions; and reduce legal and financial liability.

8.3 Privacy Impact Assessment Principles

Each PIA shall assess whether the proposed initiative has a lawful authority, demonstrates a necessary and proportionate purpose, minimizes privacy impacts, uses the least privacy-invasive approach available, includes appropriate security safeguards, establishes adequate oversight and accountability measures, and complies with applicable records management requirements.

9. WHEN A PRIVACY IMPACT ASSESSMENT IS REQUIRED

A Privacy Impact Assessment shall be completed whenever the Township proposes any new initiative or significant change involving personal information. A Privacy Impact Assessment may not be required where an initiative does not involve personal information or presents no material change to existing privacy practices, systems, or processes, such as routine administrative activities, minor system updates that do not affect privacy protections, or activities involving only publicly available information.

A PIA shall be completed before the collection of personal information, unless an exception applies under applicable legislation or regulation. A PIA shall also be updated before a significant change to the purpose for which personal information is used or disclosed, where required by law.

PIAs are required for new or substantially changed programs, systems, cloud services, AI, surveillance, websites, online services, vendors, payment systems and information-sharing initiatives. A PIA shall be completed for, but is not limited to, the following situations.

9.1 New Municipal Programs

Examples include: new municipal services, grant programs, licensing programs, volunteer management systems, public engagement platforms, citizen request systems, complaint management systems and recreation programming.

9.2 Existing Programs Undergoing Significant Change

Examples include: additional information collection, new information sharing, expanded public access, changes in legal authority, changes to retention periods, expanded staff access, automation of manual processes and integration with other systems.

9.3 Technology Projects

Examples include: software implementation, database replacement, enterprise systems, GIS systems, permitting software, payroll systems, accounting software, electronic records management, usage tracking, customer relationship management software and mobile applications.

9.4 Cloud Services

Examples include: Cloud document storage, hosted email, SaaS applications, online payment systems, hosted recreation software and hosted building permit software.

9.5 Artificial Intelligence

Examples include: generative AI, AI-assisted drafting, chatbots, predictive analytics, automated classification, automated workflow, facial recognition, voice recognition and image analysis.

9.6 Website Changes

Examples include: online forms, service portals, payment portals, customer accounts, appointment scheduling, analytics platforms, cookies, embedded mapping and social media integration.

9.7 Surveillance Technology

Examples include: CCTV, body-worn cameras, building access systems, licence plate recognition, audio recording, GPS tracking and drone technology.

9.8 Procurement

Whenever procurement involves personal information, confidential municipal information, cloud hosting, outsourcing, software implementation and managed IT services.

9.9 Information Sharing

Examples include: sharing information with neighbouring municipalities, conservation authorities, police services, provincial ministries, federal agencies, contractors, consultants, auditors and payment processors.

9.10 Human Resources

Examples include: recruitment systems, applicant tracking, payroll, benefits, employee wellness, performance management, electronic personnel files and training records.

9.11 Financial Services

Examples include: electronic payments, credit card processing, banking interfaces, taxation software, billing, accounts receivable and electronic funds transfer.

9.12 Emergency Management

Examples include: emergency notification systems, evacuation registries, vulnerable persons registries and emergency response software.

9.13 Geographic Information Systems

Where GIS information may identify: property owners, residents, complainants, infrastructure linked to individuals.

9.14 Elections

Examples include: voters' lists; electronic poll books, online candidate filing, (if implemented), campaign finance reporting and internet voting (if implemented).

10. PRELIMINARY PRIVACY SCREENING

Before initiating a full PIA, the Department Head shall complete a Preliminary Privacy Screening. (Appendix A)

The screening determines whether:

- a full PIA is required;
- an abbreviated PIA is appropriate; or
- no PIA is necessary.

The screening shall be provided to the Clerk.

11. METHODOLOGY

The PIA process generally follows four key steps.

Step 1: Preliminary Analysis Questionnaire (Appendix A)

a) Examine the project to determine if it will involve the collection, use, retention, disclosure, security or disposal of personal information.
b) Submit the completed Preliminary Analysis Questionnaire to the Clerk for review.
c) If the Clerk, or designate, determines that the project WILL involve personal information, proceed with the PIA process. If the project WILL NOT involve personal information, you do not need to proceed with the PIA process.

Step 2: Project Analysis Questionnaire (Appendix B)

a) Gather more specific information about the project, its scope and key characteristics, roles and responsibilities of parties, including third parties, the type of personal

information involved and the manner in which the personal information will be collected, used, retained, disclosed, secured or disposed of.

Step 3: Privacy Analysis (Appendix C)

a) Using information gathered in the previous step, identify MFIPPA requirements and potential risks and impacts to privacy.
b) Consider ways to reduce or eliminate the risks and impacts identified.
c) Assess proposed solutions and their relative advantages and disadvantages.

Step 4: PIA report (Appendix D)

a) Privacy Impact Assessment Report is a report that identifies privacy risks and offers recommendations to address those risks.
b) Obtain approval to proceed with recommended solutions.
c) Document your findings and chosen solutions in a PIA report.
d) Proceed with the project, ensuring that the recommendations from your PIA are fully incorporated in the project plans and implemented.

The Information and Privacy Commissioner of Ontario's Planning for Success: Privacy Impact Assessment Guide for Ontario's Public Institutions **(Appendix E)** provides guidance to institutions in conducting a Privacy Impact Assessment (PIA).

12. PIA PROCESS

Step 1 – Complete the Preliminary Analysis Questionnaire (Appendix A)

Objective: Determine whether the project involves personal information and whether a PIA is required.

Activities

- Complete a PIA Preliminary Analysis Questionnaire (Appendix A)
- Determine whether the initiative:
  - Collects personal information
  - Uses existing personal information in a new way
  - Shares information with another organization
  - Introduces new technology
  - Changes an existing business process
  - Uses artificial intelligence, analytics, cloud services, or automation
  - Involves a third-party service provider

Decision

- No personal information → No PIA required.

- Personal information involved → Proceed with the PIA.

Where a Preliminary Privacy Screening Questionnaire determines that a full Privacy Impact Assessment is not required, the Department Head shall review and acknowledge the results, ensure any identified privacy risks or recommended controls are addressed, and provide a copy of the completed screening documentation to the Clerk for recordkeeping purposes. The completed screening shall be retained in accordance with records management requirements as evidence of the privacy review undertaken and may be revisited if the scope, use, collection, disclosure, technology, or handling of personal information changes.

Step 2 – Establish the PIA Team and Complete the Project Analysis Questionnaire (Appendix B)

Objective: Assign responsibility and identify stakeholders.

Include

- Municipal Staff
- Department Head
- Privacy Officer / Records Access and Privacy Designate
- Legal Services
- Business Owner
- Records Management
- IT Lead
- Procurement (if vendors are involved)

Step 3 – Describe the Project/Scope of the PIA

Objective: Clearly explain what the project will do.

Document

- Business need
- Objectives
- Scope
- Technology involved
- Users
- Business processes
- Expected outcomes

Questions

- Why is the project needed?
- What problem is being solved?
- Who will use the system?

Step 4 – Identify Legislative Authority/Project Authority

Objective: Confirm the legal authority for collecting, using, and disclosing personal information.

Document

- Applicable legislation
- Applicable regulations
- Institutional policies
- Program authority

Questions

- What legislation authorizes the activity?
- Is the collection necessary?
- Is consent required?

Step 5 – Inventory Personal Information / Project Characteristics

Objective: Identify every type of personal information involved.

Record

- Personal identifiers
- Contact information
- Financial information
- Employment information
- Education records
- Health information (if applicable)
- Images/video
- Location data
- Device information
- Biometric information

For each information type document:

- Source
- Purpose

- Collection method
- Users
- Storage location
- Retention period

Step 6 – Map Information Flows/Roles & Responsibilities

Objective: Understand how personal information moves through the organization.

Map

Collection
↓
Use
↓
Storage
↓
Access
↓
Disclosure
↓
Retention
↓
Disposal

Include:

- Internal users
- External partners
- Vendors
- Cloud providers
- Cross-border transfers

Step 7 – Assess Compliance with Privacy Principles

Review whether the project complies with key privacy requirements.

Collection: Is only necessary information collected?

Notice: Will individuals receive proper notice?

Consent: Is consent required? How will it be obtained?

Use: Is use limited to the stated purpose?

Disclosure: Who receives the information? Is disclosure authorized?

Retention: Are retention schedules documented?

Disposal: Is secure destruction planned?

Access: Can individuals request access or correction?

Accountability: Who is responsible for the information?

Step 8 – Identify Privacy Risks & Complete the Privacy Analysis Checklist (Appendix C)

Objective: Identify risks to individuals and the organization.

Consider:

- Over-collection
- Unauthorized access
- Inappropriate disclosure
- Weak authentication
- Insider threats
- Third-party risks
- Cloud storage
- Artificial intelligence
- Excessive retention
- Data quality issues
- Inadequate transparency
- Lack of audit logging

For each risk assess:

- Likelihood
- Impact
- Overall risk rating

Step 9 – Identify Privacy Controls

Administrative Controls

- Privacy policies
- Staff training
- Confidentiality agreements
- Privacy notices
- Vendor contracts
- Records retention schedules

Technical Controls

- Encryption
- Multi-factor authentication
- Role-based access
- Logging
- Monitoring
- Data masking
- Secure backups
- Antivirus and endpoint protection
- Secure networks

Physical Controls

- Locked facilities
- Visitor controls
- Secure storage
- Secure destruction
- Surveillance systems
- Alarm systems
- Environmental controls for records storage
- Controlled access to server rooms
- Protection of workstations and devices

Step 10 – Develop Risk Mitigation Strategies

For every identified risk:

Document:

- Risk
- Recommended control
- Responsible owner
- Completion date
- Residual risk

Example

Risk	**Mitigation**	**Owner**
Excessive collection	Remove unnecessary fields	Business Lead
Unauthorized access	Implement MFA	IT
Vendor risk	Complete vendor privacy review	Procurement

Step 11 – Complete the PIA Report

The IPC recommends documenting the assessment in a comprehensive report that includes:

- Executive Summary
- Project Description
- Legislative Authority
- Personal Information Inventory
- Information Flows
- Privacy Analysis
- Security Analysis
- Risk Assessment
- Risk Mitigation Plan
- Residual Risks
- Recommendations
- Appendices

The Department Head, in consultation with the Clerk and/or Privacy Officer (Records Access and Privacy Designate) where appropriate, shall determine whether a formal PIA report is required based on the complexity, scope, and privacy risks associated with the initiative.

For initiatives that present low to moderate privacy risk, a separate formal PIA report may not be required, provided that the **PIA Screening Questionnaire**, **Project Analysis Questionnaire**, and **Privacy Analysis Checklist** have been fully completed, accurately document the assessment, identify any privacy risks and mitigation measures, and provide sufficient information to support decision-making and demonstrate compliance with applicable privacy legislation and this policy.

Where the initiative involves significant privacy risks, sensitive personal information, new or emerging technologies, substantial changes to business processes, information sharing with external organizations, or other circumstances identified by the Department Head, Clerk, Privacy Officer or Records Access and Privacy Designate, a comprehensive PIA report shall be prepared and submitted to the Clerk for review and approval prior to implementation.

Step 12 – Review and Obtain Approvals

Review with:

- Privacy Officer / Records Access and Privacy Designate
- Chief Administrative Officer/IT
- Legal Counsel (if applicable)
- Business Owner
- Executive Sponsor

Document:

- Outstanding issues
- Accepted risks
- Required actions
- Final approval

Step 13 – Implement Privacy Requirements

Before implementation:

- Complete required mitigation actions.
- Update policies and procedures.
- Configure technical controls.
- Train staff.
- Update privacy notices.
- Execute vendor agreements.
- Confirm records retention requirements.

Step 14 – Monitor and Maintain

A PIA is a living document. The Township shall review PIAs periodically, or more frequently where warranted by changes in legislation, technology, operations, privacy risks, or information practices. Significant privacy breaches may trigger a review or update of the associated Privacy Impact Assessment.

Review the PIA when:

- New personal information is collected
- Business processes change
- Technology changes
- A new vendor is engaged
- New legislation comes into effect
- A privacy breach occurs
- Significant changes are made to the project

Process Flow

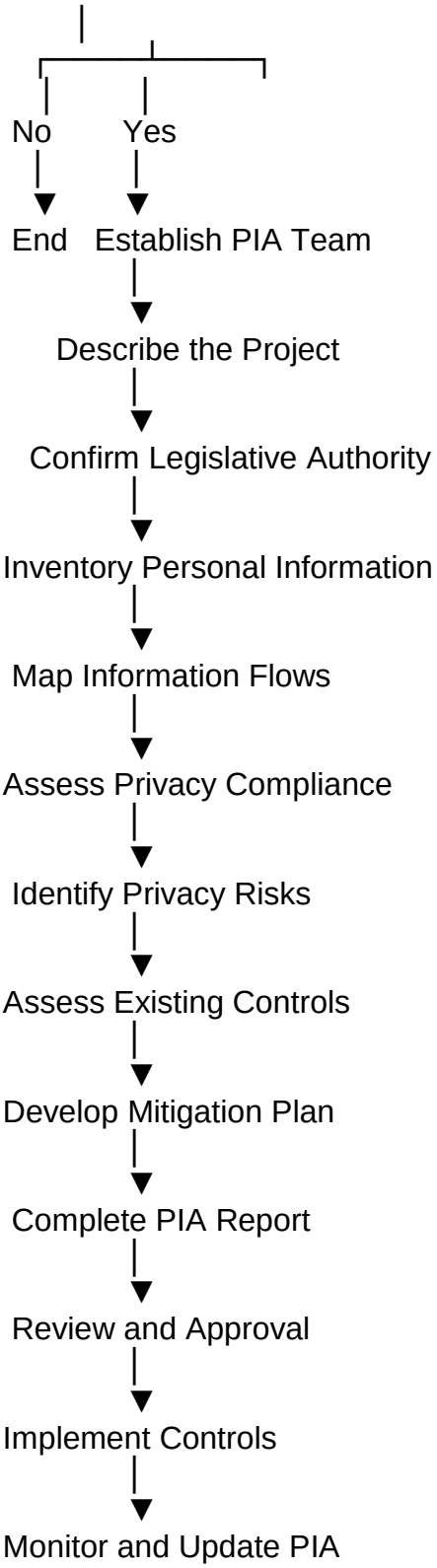
Project Proposed

▼

PIA Screening

▼

PIA Required?


No
Yes
End
Establish PIA Team
Describe the Project
Confirm Legislative Authority
Inventory Personal Information
Map Information Flows
Assess Privacy Compliance
Identify Privacy Risks
Assess Existing Controls
Develop Mitigation Plan
Complete PIA Report
Review and Approval
Implement Controls
Monitor and Update PIA

13. PRIVACY PROTECTION REQUIREMENTS

All projects, programs, services, technologies, and business processes involving personal information shall comply with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), this Policy, and the principles of Privacy by Design.

Departments shall ensure that personal information is collected, used, disclosed, retained, and disposed of only where authorized by law and only to the extent necessary to achieve a lawful municipal purpose. Appropriate administrative, technical, and physical safeguards shall be implemented throughout the information lifecycle. Privacy risks shall be identified and addressed through the Privacy Impact Assessment process prior to implementation whenever required.

14. TECHNOLOGY ASSESSMENTS

New or significantly modified information technology, digital services, software, cloud solutions, surveillance technologies, artificial intelligence, or other systems involving personal information shall undergo appropriate privacy and security assessments before implementation.

Assessments shall consider legal authority, information flows, security safeguards, vendor arrangements, data residency where applicable, records management requirements, and compliance with applicable legislation, policies, and standards.

15. ARTIFICIAL INTELLIGENCE

The use or implementation of Artificial Intelligence (AI) systems involving personal information shall require a Privacy Impact Assessment and any other applicable technology or security assessments before implementation.

Departments shall ensure AI is used lawfully, transparently, and responsibly, with appropriate human oversight. Assessments shall consider privacy impacts, data quality, bias, fairness, security, and risks associated with automated decision-making. Additional review may be required where significant risks are identified.

16. CLOUD COMPUTING

Cloud services that collect, use, disclose, store, or process personal information shall be assessed before implementation to ensure appropriate privacy and security safeguards are in place.

Departments shall consider data residency, contractual protections, access controls, business continuity, vendor responsibilities, breach notification requirements, and secure retention and disposal of information.

17. THIRD PARTY VENDORS

Departments engaging third-party service providers that collect, use, disclose, store, or process personal information shall conduct appropriate due diligence based on the sensitivity of the information and the level of risk.

Where appropriate, agreements shall include provisions respecting confidentiality, authorized use and disclosure, security safeguards, incident reporting, audit rights, and the return or secure disposal of personal information upon termination of the service. Any significant residual privacy risks shall be documented and managed through the Privacy Impact Assessment process.

18. WEBSITE AND ONLINE SERVICES

Websites, online services, portals, applications, and other digital services that collect, use, disclose, or process personal information shall be designed and operated in accordance with applicable privacy legislation and the principles of Privacy by Design. Departments shall collect only the personal information necessary to provide the service, provide appropriate privacy notices, and implement suitable safeguards. New or significantly modified online services involving personal information shall be assessed through the Privacy Impact Assessment process before implementation.

19. SURVEILLANCE TECHNOLOGIES

The acquisition, implementation, or use of surveillance technologies shall be lawful, necessary, proportionate, and consistent with this Policy. Departments shall assess privacy risks before implementation and complete a Privacy Impact Assessment where required.

20. INFORMATION SHARING

Personal information shall be shared only where authorized by law and necessary for a legitimate municipal purpose. Departments shall limit information sharing to the minimum necessary, implement appropriate safeguards, and complete a Privacy Impact Assessment where information-sharing arrangements present significant privacy risks.

21. DATA MINIMIZATION

Departments shall collect, use, retain, and disclose only the minimum amount of personal information necessary to achieve an authorized municipal purpose. Information holdings shall be reviewed periodically to eliminate unnecessary or outdated personal information.

22. SECURITY SAFEGUARDS

Departments shall implement administrative, technical, and physical safeguards appropriate to the sensitivity of the personal information being managed. Safeguards shall be reviewed periodically to address changing risks and protect personal information throughout its lifecycle.

23. RECORDS MANAGEMENT & GOVERNANCE

Records containing personal information shall be managed throughout their lifecycle in accordance with applicable legislation, the Township's Records Retention By-law, and approved records management practices. Access shall be limited to authorized individuals, and completed Privacy Impact Assessments shall be retained in accordance with approved retention requirements.

The Township shall maintain governance practices that establish clear accountability, oversight, and responsibilities for privacy management, support compliance with applicable legislation, and promote ongoing monitoring and continuous improvement.

24. TRAINING

The Chief Administrative Officer, or designate, shall ensure that employees and others who handle personal information receive appropriate privacy and information management training. Training shall be provided upon hire, periodically thereafter, and whenever significant legislative, technological, or operational changes occur.

25. REVIEW

This Policy shall be reviewed periodically by the Clerk/Privacy Officer or Records Access and Privacy Designate to ensure continued alignment with applicable legislation, Information and Privacy Commissioner of Ontario guidance, technological developments, and municipal privacy practices.

26. EFFECTIVE DATE

This policy comes into effect on the date approved by Council.

Appendix A: Preliminary analysis questionnaire

1. Project and institution

PROJECT TITLE	
INSTITUTION	
DEPARTMENT	
PROJECT LEAD	

2. PIA lead

NAME AND TITLE	
INSTITUTION	
DEPARTMENT	
PHONE NUMBER	
E MAIL	

3. Project description

Describe the project (for example, the program, system, application or activity) that is the subject of the PIA, including its purpose, scope, and key objectives. Attach relevant project documentation, if necessary.

4. Collection, use and disclosure

4.1 Identify the kinds of information involved in the project (check all that apply).

	YES	NO	UNKNOWN
Information about individuals in their personal capacity			
Information about individuals acting in their business, professional or official capacity (for example: name, job title, and business contact information)			
Information about institutions (for example: for profit and not-for-profit institutions and government institutions)			
Aggregated or de-identified information. In the row below, outline the process followed to aggregate or de-identify the information and the potential to identify/ re-identify individuals from that information.			

4.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
No personal information						
Unknown at this time (please explain why in row below.)						
In the rows below, list the types of personal information involved in the project (add more rows as needed). If third parties will be involved in the project, think about what they may be doing with personal information as well.						
In the rows below, list each element of non-personal information that, when combined or linked, may enable identification of an individual (add rows as necessary).						

4.3 To whom does the personal information relate? List the individuals whose personal information will be involved in the project (in other words, the data subjects).

5. Privacy Legislation

5.1 Identify applicable privacy legislation (check all that apply).[1]

	YES	NO	UNKNOWN
Freedom of Information and Protection of Privacy Act			
Municipal Freedom of Information and Protection of Privacy Act			
None or other (Please explain below.)			

5.2 Public records and excluded personal information[2]

	YES	NO	UNKNOWN
Does the project involve any personal information that will be maintained for the purpose of creating a record that is available to the general public? What is the type of personal information, and why and how is it made available to the general public? Please explain in the row below.			
Does the project involve any personal information that will be excluded from the application of the acts by section 65 of FIPPA and section 52 of MFIPPA? What is the type of personal information, and why is it excluded? Please explain in row below.			

[1] See the ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** for information about conducting a PIA involving personal health information regulated under that act.

[2] Consult with your legal and privacy staff to determine if you should continue with the PIA process, and if other legislation or policies define privacy requirements that must be complied with.

6. Conclusion

Indicate whether you will proceed with the PIA process and the reasons for your decision. (Institutions must complete a written PIA before collecting personal information, unless a regulatory exception applies.)

Appendix B: Project analysis questionnaire

1. Scope of PIA

Define the scope of the PIA review and analysis. What aspects of the project are in and out of scope?

2. Project authority

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understanding, agreements, contracts and other relevant instruments).

3. Project characteristics

3.1 Identify key characteristics of the project (check all that apply).

DOES THE PROJECT INVOLVE…	YES	NO	UNKNOWN
creating a new program, process, service, technology, information system or other type of IT application?			
a change to an existing program, process, service, technology, information system or other type of IT application?			
a new collection of personal information?			
procuring goods or services?			
outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information?			
developing a request for bids, proposals, or services?			
a process, system or technology for which the privacy risks are not known or well documented?			
creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases?			
information sharing (internal and external)?			
the need to identify, authenticate or authorize users – including public and/or internal staff?			
other activities that may impact privacy? (Please explain below.)			

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed project analysis questionnaire.

3.3 Identify any changes that will result from the project (check all that apply).

WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change in business owner?			
a change to legislative authority?			
a change in users (internal and external) of a related process or system?			
a change in partners or service providers (internal and external)?			
a change in the amount, type of, or ways that personal information is collected, used, disclosed, retained, secured or disposed of?			
a change to the purposes for which personal information will be collected, used, or disclosed?			
a change from direct to indirect collection of personal information?			
a change in roles and responsibilities (such as who can do what, when, where, why and how with personal information)?			
a change to, or elimination of, existing practices of de-identifying information?			
a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information (for example: hardware and software)?			
a change to an information system or database containing personal information?			
a change of medium or service delivery channels (for example: the automation of manual processes, conversion from paper to electronic records, or the			

creation of a new website to provide services to clients)?			
WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change in the security requirements or safeguards, practices, or measures?			
other changes (please specify change or proposed change below)?			

3.4 If you answered yes to any of the above, explain the change(s), including what specifically will change and why it is necessary. Attach all relevant documentation to your completed project analysis questionnaire.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

4. Technology

4.1 Identify technology-related characteristics of the project (check all that apply)**.**

DOES THE PROJECT INVOLVE…	YES	NO	UNKNOWN
technology designed to monitor, track or observe an individual or their transactions (for example: video cameras, cell phones, and geospatial or location-based services)?			
logging information, usage or preferences (for example: IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology)?			
public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media?			
using analytics or performance measurements (for example: web analytics, social media analytics, or business intelligence tools)?			
processing or storing of personal information in a virtual environment (for example, cloud computing)?			
acquiring or customizing commercial software, hardware, or IT support services by external vendors?			
developing or customizing software, hardware, or IT support services in-house?			
creating information systems or other types of IT applications that will be populated by others (for example, clients of a system or service will supply information)?			
a system or application that will automatically collect, use, disclose or retain personal information?			
other (Please explain below.)			

4.2 If you answered yes to any of the above, provide an explanation of the technology (that is, purposes, why necessary and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

5. Roles and responsibilities

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role.

INSTITUTION/THIRD PARTY	PROJECT ROLE

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose secure or dispose of personal information <u>on behalf</u> of your institution.

INSTITUTION/ THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE

5.3 Identify any location outside of Ontario where personal information may be retained or stored and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY

5.4 List all position titles of the officers, employees, consultants, or agents of your institution who will have access to the personal information. For example, program area staff (by title), IT staff, legal counsel, etc.

PARTY	RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5 Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
contracts				
memoranda of understanding				
agreements (service level and trade)				
other (Please explain below.)				

6. Relevant information

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed project analysis questionnaire.

7. Personal information flows

Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your identified flows of personal information throughout the project to your completed project analysis questionnaire.

Appendix C: Privacy analysis checklist

Answering the following questions can help you to identify the privacy risks that need to be addressed and the steps to be taken to ensure compliance with FIPPA or MFIPPA. You can use the table below to organize your work, or it can be adapted to meet the needs of the project and your institution. Be sure to address all the identified questions and consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all the types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y[3]	N[4]	IP[5]	NA[6]	EXPLANATION		
Review each question and determine how each relates to the project. **Note:** Do not use the checklist as a substitute for the legislation. The statutory provisions have been summarized here.	Put a check mark (√) in the appropriate column for each question. This will create a visual representation of the project to assist with complying with FIPPA or MFIPPA. If your findings differ depending upon the type of personal information involved, add rows to document and explain the differences for each type.				Outline how you arrived at your findings. Provide as much information as is available, particularly if action is planned, but not yet implemented. Outline any options or alternatives that were, or need to be, considered. Explain why no action has been taken or planned for each "N" finding, and why requirements are "NA" to the project.	For each finding, outline the potential impact or risk to privacy. For example: a theft, loss or unauthorized use or disclosure of the personal information, non-compliance with FIPPA or MFIPPA, increased intrusiveness into the private lives of individuals, or it does not meet the public's expectation of privacy.	For each finding, identify the action(s) (steps) necessary for compliance with the privacy requirement or to mitigate or prevent a potential privacy impact or risk.

[3] **Y (Yes):** You know the privacy protection requirement either has been met by existing safeguards, practices or measures or will be met by action planned before implementation

[4] **N (No):** You know nothing has been done or is planned to address this privacy protection requirement; there is a possible privacy risk and "gap" in the project's compliance. If nothing has been done or planned, explain why.

[5] **IP (In Progress):** You do not know the answer to the question at this time; more information or analysis is required and, until such time, there is a potential privacy risk and gap.

[6] **NA (Not Applicable):** You know this privacy protection requirement is not applicable to the project. Note: Be sure to check with your FIPPA or MFIPPA Coordinator and Legal Counsel.

A. Collection

Key requirements:

- A written PIA report must be prepared before collecting personal information.
- For each collection of personal information, ensure that the institution collects personal information only if it has the authority to do so. Consider the following:
    - Is the collection expressly authorized by statute?
    - Will the personal information be used for law enforcement purposes?
    - Is the collection necessary for the proper administration of a lawfully authorized activity?
    - Why is personal information necessary to achieve the purpose of the collection?
- Personal information must be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or other statutory provision.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- Risk prevention and mitigation steps must generally be implemented by the institution before collecting personal information.
- See sections 28 and 29 of MFIPPA and sections 38 and 39 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Is the collection of personal information authorized under FIPPA or MFIPPA or another act?							
Do all parties collecting personal information have legal authority for the collection?							
Have you documented the legal authority for the intended collection?							
Has responsibility for the collection been assigned to program staff or third party service providers?							
PURPOSE OF COLLECTION							
Has each purpose of the collection been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
NOTICE TO INDIVIDUAL							
Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.							
Will the notice of collection comply with FIPPA or MFIPPA? Explain how or if there are missing components.							
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the types, sources and form of collection.							
Will personal information be collected indirectly from another source, or covertly? Why?							
Will indirect collection comply with FIPPA or MFIPPA? Explain the authority for indirect collection.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
CONTROLS							
Will the project only collect personal information for which there is legal authority?							
Will there be any limitations or restrictions imposed on the collection of the personal information?							
Will there be periodic reviews of the collection controls to ensure effectiveness?							
DATA MINIMIZATION							
Is personal information necessary for the project to proceed?							
Is collection of all the personal information necessary? Why or why not?							

B. Use

Key requirements:

- For each use of personal information, ensure that all parties involved in the project, including your institution, partners and other third parties, use personal information only with the authority to do so. Consider the following:
    - Is the use for the purpose it was collected or for a consistent purpose?[7]
    - Is the use authorized by the individual to whom it relates?
    - Does the use comply with another statute?
    - Is the use for other purposes permitted by FIPPA or MFIPPA?
    - Why is personal information necessary to achieve the purpose of the use?
- Before making any significant change to a purpose for which personal information is used, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 31 of MFIPPA and sections 38 and 41 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?							
Have you documented the legal authority for the intended use(s)?							

[7] A consistent purpose is a use of personal information that the individual to whom the personal information relates might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
PURPOSE(S) OF USE							
Has each purpose of use been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be used for other purposes?							
Will uses of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF USE							
Have all parties using personal information been defined by position title (for example: program staff, consultants, agents of the institution, third party service providers, employees, officers etc.)?							
Have you indicated how each type of personal information will be used?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
CONTROLS							
Will there be administrative, technical, and physical safeguards, practices, and measures in place to ensure personal information will be used only for authorized purposes and by authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the use(s) of the personal information?							
Will there be periodic reviews of the use safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is use of all the personal information necessary for the project to proceed? Why or why not?							

C. Disclosure

Key requirements:

- For each disclosure of personal information, ensure that all parties involved in the project disclose personal information only with the authority to do so. Consider the following:
    - Is the disclosure for the purpose for which it was collected or for a consistent purpose?[8]
    - Is the disclosure authorized by the individual to whom the personal information relates?
    - Does the disclosure comply with another statute?
    - Is the disclosure for other purposes permitted by FIPPA or MFIPPA?
    - Why is the personal information necessary to achieve the purpose of the disclosure?
- Before making any significant change to a purpose for which personal information is disclosed, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 32 of MFIPPA and sections 38 and 42 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
Have you documented the legal authority for the intended disclosures?							

[8] A consistent purpose is a disclosure of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
PURPOSE(S) OF DISCLOSURE							
Has each purpose of disclosure been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be disclosed for other purposes?							
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined (for example: program staff, consultants, agents, third party service providers, employees, officers, etc.)?							
Have you indicated how each type of personal information will be disclosed?							
Has the manner of disclosure been defined (for example: oral, mail, email, etc.)?							
Will the disclosures be documented and how?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?							
CONTROLS							
Will there be administrative, technical and physical safeguards, practices and measures in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the disclosures of the personal information?							
Will there be periodic reviews of the disclosure safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[9]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[10]							

[9] Before such a disclosure, there should be a defined and documented process that makes sure the researcher demonstrates why identifiable information is required for the research purpose. The researcher must agree to the terms and conditions of Ontario Regulations 460 and 823, section 10.

[10] FIPPA defines when disclosure of personal information by educational institutions or hospitals may be done for fundraising purposes. Before such disclosures, ensure the requirements, as defined in sections 42(2) and (3), have been met.

D. Accuracy and correction

Key requirements:

- Take reasonable steps to ensure personal information is not used or disclosed unless it is accurate, complete and up to date.
- Ensure that every individual can:
  - correct their personal information
  - have a statement of disagreement attached to the personal information if the correction is not made
  - require a notice of the correction or the statement of disagreement to be sent to anyone to whom the personal information was disclosed within the year before the above action was taken
- See sections 30(2) and 36 of MFIPPA and 40(2) and 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
STANDARD OF ACCURACY							
Will there be measures in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of measures.							
CORRECTING THE PERSONAL INFORMATION							
Will there be a defined and documented process for the processing of a request for the correction of personal information? Provide details of process.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
CORRECTION REQUESTS/STATEMENT OF DISAGREEMENT							
Will there be a defined and documented process for individuals to request the correction of their personal information? Provide details of the process.							
CONTROLS							
Will controls be in place to ensure that only authorized personnel will be able to add, change, or delete personal information?							
Will there be periodic reviews of the controls to ensure effectiveness?							

E. Security

Key requirements:

- Take all reasonable measures to prevent unauthorized access to personal information in your custody or control, taking into account the nature of the record to be protected.
- Access should be restricted to only those individuals who need the personal information for the performance of their duties.
- Explain the safeguards, practices and measures that will be used to protect the personal information.
- Summarize any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of personal information
- Take all reasonable safeguards, practices and measures to protect personal information against loss or theft, unauthorized access, use or disclosure, inadvertent modification, destruction or damage, taking into account the format of the record to be protected.
- See Ontario Regulation 823, section 3 as well as sections 28 and 30(5) of MFIPPA, and Ontario Regulation 460, sections 3 and 4, as well as sections 38 and 40(5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
SECURITY MEASURES							
Will safeguards, practices and measures be used to protect the personal information? Explain each administrative, technical and physical safeguard, practice and measure.							
Will risk prevention and mitigation steps be implemented before collecting the personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
CONTROLS							
Will security safeguards, practices and measures be defined and documented to protect the confidentiality, integrity and availability of personal information?							
Will testing and periodic reviews be conducted to ensure that personal information is only collected, accessed, used, disclosed, retained and disposed of when authorized and is not stolen or lost?							
Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?							
Will procedures be defined and documented on how to identify, report, investigate and address the theft, loss and/or unauthorized access, collection, uses and/or disclosure of personal information?							



F. Requesting access to personal information

Key requirements:

- Ensure that every individual has a right of access to their personal information in the institution's custody or control.
- Make sure that personal information in the institution's custody or control is retrievable.
- Verify the identity of persons requesting access to their personal information.
- See section 36 of MFIPPA and section 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCESS REQUESTS							
Will the management of personal information change or restrict individuals' right of access to their personal information?							

G. Retention

Key requirements:

- Personal information should be retained for at least one year after use to provide the individual with a reasonable opportunity to access their personal information.
- The individual's consent should be obtained in order to dispose of personal information prior to one year after use.
- Ensure compliance with other relevant records retention laws, regulations, bylaws or other requirements.
- See MFIPPA sections 28(3), 30(1), 30.1(8) and Ontario Regulation 823, section 5; FIPPA sections 38(3), 40(1), 40.1(8) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
RETENTION SCHEDULES							
Will there be defined and documented policies, procedures, and other requirements related to the retention of personal information?							
REASONABLE OPPORTUNITY FOR ACCESS							
Will safeguards, practices and measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
MEDIUM AND LOCATION OF RETENTION							
Has the medium and format of the personal information to be retained been defined?							
RETENTION PERIOD							
If the personal information has not been used, will it be retained for only as long as necessary to meet its purpose? How long will it be retained?							
How long will personal information that has been used be retained?							
CONTROLS							
Will procedures be defined and documented related to consent for early disposal of personal information?							
Will there be periodic reviews of the retention requirements and consent procedures to ensure effectiveness?							



H. Disposal and destruction

Key requirements:

- Personal information must be disposed by either securely destroying it or transferring it to the appropriate archives.
- Make sure personal information is only destroyed when authorized by an appropriate party and in accordance with records retention laws/regulations/bylaws applicable to the institution.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be destroyed throughout the process, that is, when personal information is stored, transported, handled and destroyed.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be transported to archives throughout the process, that is, when personal information is stored, transported and handled.
- Take all reasonable safeguards, practices and measures to destroy personal information so it cannot be reconstructed or retrieved.
- Keep an accurate record of the disposal, including what personal information was destroyed or transferred and on what date it was destroyed or transferred.
- Do not include personal information in your record of disposal.
- See Ontario Regulation 823 and section 30(4) and (5) of MFIPPA, and Ontario Regulation 459 and sections 40(4) and (5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
MANNER OF DISPOSAL							
Will procedures be defined and documented for the secure disposal, for example, transfer to archives or destruction of personal information in accordance with applicable records retention schedules, laws/ regulations/ bylaws? Explain the disposal process.							
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							
CONTROLS							
Will safeguards, practices and measures be defined and documented to ensure only appropriate personal information will be disposed of or destroyed, and only by authorized parties after obtaining appropriate approval?							
Will there be periodic reviews of the disposal safeguards, practices and measures to ensure effectiveness?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
RECORD-KEEPING							
Will details of the disposal of personal information be recorded?							
Will safeguards, practices and measures be defined and documented to ensure no personal information is captured in the disposition record?							

I. Privacy management

The questions in this section relate to privacy management throughout your institution. They are not limited to the project's information system, technology, or program, but address your institution's privacy maturity, capability, and readiness to undertake the project.
The emphasis is on accountability and training.

Key requirements:

- Apply common management principles, such as planning, directing, controlling and evaluating the personal information collected, used, disclosed, retained and destroyed by institutions.
- Establish and follow disciplined and consistent practices for the management of personal information.
- Educate staff about privacy, as well as legislative and other relevant requirements.
- Periodically review safeguards, practices, and measures, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCOUNTABILITY							
Will accountability for managing personal information throughout its lifecycle be defined to include parties involved in the project (for example: your institution, **officers, employees, consultants or agents of your institutions**, partners, vendors and other third parties)? Explain accountability.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
TRAINING							
Will operational safeguards, practices, and measures related to the protection of personal information be needed?							
Have all parties requiring training on operational, security, and privacy aspects of the project been identified?							
Has the individual responsible for ensuring that all parties receive appropriate training been identified?							
AUDITS							
Will safeguards, practices, and measures be developed and documented to evaluate whether the personal information is accessed, collected, used, retained, disclosed, secured, and disposed of in a manner that is consistent with FIPPA or MFIPPA, or if it is stolen or lost?							



Appendix D: PIA report template

Mandatory information to be contained in a PIA

As of July 1, 2025, under FIPPA and January 1, 2027, under MFIPPA, PIAs are mandatory before collecting personal information (subject to any prescribed exceptions) and must contain, at minimum, the information set out in section 38 of FIPPA or section 28 of MFIPPA:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.
3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended to be collected.
5. The position titles of the officers, employees, consultants, or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use, or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40(1) of FIPPA or 30(1) of MFIPPA.
8. An explanation of the administrative, technical and physical safeguards, practices and measures that would be used to protect the personal information in accordance with subsection 40(5) of FIPPA or 30(5) of MFIPPA and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,
    i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    ii. to mitigate the risks to individuals in the event of such an occurrence.
10. Such other information as may be prescribed.

Risk prevention and mitigation steps outlined in the PIA must generally be implemented before collecting personal information. It is important that you review both new and existing legal requirements when preparing your PIA report and ensure that it includes all required information.[11]

[11] See PIA requirements in section 38 of FIPPA and section 28 of MFIPPA.



Privacy Impact Assessment Template

Initiative Information	
Initiative Name:	
Institution:	
Program / Service Area:	
Initiative Description:	

Assessment Information	
PIA Status	*Initial PIA / Updated PIA*
Related / Previous PIA, if applicable	
Prepared By:	
Reviewed By:	
Approved By:	
Date Approved:	
PIA Version:	

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.

2. The legal authority for the intended collection, use and disclosure of the personal information.

3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.

Type of Personal Information	Intended Use(s)	Intended Disclosure(s)

4. The sources of the personal information that is intended to be collected.



5. The position titles of the officers, employees, consultants or agents of the institution who will have access to the personal information.

Position Title	Department / Business Area	Personal Information / Type Accessed	Reason Access Required	Access Limitations, if applicable

6. Any limitations or restrictions imposed on the collection, use or disclosure of the personal information.

Limitations on Collection

Limitations on Use

Limitations on Disclosure

7. The period of time that the personal information would be retained by the institution, in accordance with subsection 30 (1).

Record Containing Personal Information	Retention Period	Source of Retention Period	Disposition

8. An explanation of the administrative, technical and physical safeguards and practices that would be used to protect the personal information in accordance with subsection 30 (5) and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.

Administrative Safeguards

Technical Safeguards

Physical Safeguards

Risks to Individuals

9. The steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and to mitigate the risks to individuals in the event of such an occurrence.

Risk Identified	Step to be Taken	How the Step Addresses the Risk	Implementation Timing

10. Such other information as may be prescribed.

Additional resources

Ontario privacy legislation, regulations, and other guidance

The *Freedom of Information and Protection of Privacy Act* (FIPPA)

- ***The Freedom of Information and Protection of Privacy Act***
- **Disposal of Personal Information – R.R.O. 1990, Reg. 459**
- **General – R.R.O. 1990, Reg. 460**

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)

- ***The Municipal Freedom of Information and Protection of Privacy Act***
- **General – R.R.O. 1990, Reg. 823**
- **Institutions – R.R.O. Reg. 372/91**

Other IPC guidance

- ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***
- ***De-identification Guidelines for Structured Data***
- ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act***

PIA guidance from other sources and jurisdictions

- Government of Ontario, ***Freedom of Information and Protection of Privacy Manual***
- Government of Ontario Recordkeeping, Access and Privacy Advisory Services at 416-327-1600 or **access.privacy@ontario.ca**
- United Kingdom Information Commissioner's Office, **Data protection impact assessments** (2023)
- Office of the Australian Information Commissioner, **Guide to Undertaking PIAs** (2021)
- United States Department of Justice, **Impact Assessment Guidance**

AUGUST 2026

Appendix E to Policy ADM-017 -
By-law 69-2026 -

Planning for Success: Privacy Impact Assessment Guide for Ontario's Public Institutions



Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

This guidance by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws and advance best practices. It should not be relied upon as a substitute for the legislation itself or as legal advice. It does not bind the IPC, which may be called upon to independently investigate and/or decide an issue based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

Contents

Introduction 1

Background 2

Methodology 6

1. Preliminary analysis 7

2. Project analysis 9

3. Privacy analysis 15

4. PIA report 19

Appendix A:
Preliminary analysis
questionnaire 23

Appendix B:
Project analysis questionnaire 28

Appendix C:
Privacy analysis checklist 37

Appendix D:
PIA report template 62

Appendix E:
Additional resources 68

Document History

Publication Date	Document Title	Description of Changes
August 2026	Planning for Success: Privacy Impact Assessment Guide for Ontario's public institutions	Updated to incorporate the statutory requirements of MFIPPA in force effective January 1, 2027.
November 2025	Planning for Success: Privacy Impact Assessment Guide for Ontario's public institutions	Updated to incorporate the statutory requirements of FIPPA in force effective July 1, 2025, and to reflect current guidance, terminology, and resources.
May 2015	Planning for Success: Privacy Impact Assessment Guide	Initial publication

Introduction

This guide is intended for institutions subject to Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) or *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). It is meant to help institutions conduct a privacy impact assessment (PIA) in accordance with these laws and best practices.[1]

The guide provides institutions with step-by-step advice on how to do a PIA from beginning to end. It will complement and support any existing requirements for PIAs that are unique to your institution. You should consult with staff responsible for privacy, project development, and risk management within your institution to ensure you comply with any additional legal or policy requirements that may apply.[2] The guide can also serve as a starting point for your institution to develop or update its own PIA methodology and processes.

For the purposes of this guide, project refers to any work involving the collection, use, retention, disclosure, security, and disposal of personal information. This may include a new program, process, service delivery model, or information technology system, or changes to an existing program, process, or system.

Comments or questions

The Information and Privacy Commissioner of Ontario welcomes your comments or questions about this guide. Please direct them to **info@ipc.on.ca** or 416-326-3333/1-800-387-0073 (within Ontario).

1 The IPC's ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** provides information on how to conduct a PIA involving personal health information regulated under that act.

2 For example, Ontario ministries and agencies are subject to requirements under numerous directives, policies and standards, such as those related to recordkeeping, access and privacy, procurement, information technology, and cybersecurity.

Background

Mandatory privacy impact assessments (PIAs) under FIPPA and MFIPPA

- **PIAs are expressly mandatory for all institutions subject to Part III of FIPPA as of July 1, 2025. PIAs are expressly mandatory for all institutions subject to MFIPPA as of January 1, 2027.**[3] Institutions must complete a written PIA before collecting personal information to evaluate privacy and security risks and outline prevention and mitigation steps, **unless a regulatory exception applies**.[4]
- The new PIA requirements apply to both recorded and unrecorded personal information.[5]
- PIAs must be done in writing, and contain, at minimum, the mandatory information set out in FIPPA and MFIPPA,[6] which includes:
  - the purpose for collecting, using or disclosing personal information and an explanation of why the personal information is necessary to achieve that purpose
  - the legal authority that the institution is relying on to collect, use or disclose the personal information
  - the types of personal information to be collected and, for each type, how it is intended to be used or disclosed
  - the sources of the personal information to be collected
  - the position titles of the institution's officers, employees, consultants or agents who will have access to the personal information
  - any limitations or restrictions imposed on the collection, use or disclosure of the personal information
  - the period of time that the personal information will be retained by the institution
  - an explanation of the administrative, technical and physical safeguards that would be used to protect the personal information and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information
  - the steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information, and to mitigate risks to individuals in the event of such a privacy breach

3 See sections 38(3)-(6) of FIPPA and sections 28(3)-(6) of MFIPPA. There are also specific PIA requirements for data integration units under Part III.1 of FIPPA. This guidance document is not a substitute for those requirements.

4 Future regulations made by the Lieutenant Governor in Council under FIPPA or MFIPPA may provide for exceptions to the requirement to complete a PIA before collecting personal information. As of the date of publication of this updated guidance, the government has not enacted any such regulations.

5 Sections 38(1) of FIPPA and 28(1) of MFIPPA, which apply to the PIA requirements in sections 38(3)-(6) of FIPPA and 28(3)-(6) of MFIPPA, expand the acts' general definition of personal information to include unrecorded personal information.

6 See section 38(3) of FIPPA and 28(3) of MFIPPA. Exceptions and additional information to be included in PIAs may also be prescribed in regulation. As of the date of publication of this updated guidance, the government has not enacted any such regulations.

- The steps set out in the PIA to prevent and mitigate risks must generally be implemented before collecting personal information.[7]
- Prior to making any significant change to the purpose for which the personal information is used or disclosed, institutions must update their PIAs and implement any additional steps necessary to prevent and mitigate risks subject to prescribed exceptions.[8]
- Institutions are required to provide the Information and Privacy Commissioner of Ontario with PIAs upon request.[9]

7 See section 38(4) of FIPPA and 28(4) of MFIPPA.
8 See section 38(5) of FIPPA and 28(4) of MFIPPA.
9 See section 38(6) of FIPPA and 28(4) of MFIPPA.

Why conduct a PIA?

A PIA is a risk management tool used to anticipate and address the potential privacy risks or impacts of a new or modified collection, use or disclosure of personal information, or of a proposed or existing information system, technology, program, process or other activity. Many institutions' policies require PIAs for projects involving personal information. For institutions subject to sections 38(3)-(6) of FIPPA or 28(3)-(6) of MFIPPA, conducting a PIA is a legal requirement that must be fulfilled before collecting personal information, subject to any exceptions set out in regulation.

Privacy risks or impacts fall into two broad categories:

- **Risks to individuals**, including the theft, loss, or unauthorized use or disclosure of personal information, which may lead to identity theft and other forms of fraud, adverse impacts on employment or business opportunities, damage to reputation, embarrassment, distress, or financial loss.
- **Risks to institutions**, including the financial, legal, and reputational impacts of privacy breaches, and the consequences of failing to comply with FIPPA and MFIPPA.

Carrying out a PIA does not need to be complex or time consuming, but thoroughness is necessary to ensure that potential privacy risks are identified and mitigated. The complexity of a PIA and the resulting documentation will depend on the complexity of the project and your institution's needs.

The benefits of conducting a PIA may include:

- meeting the legal requirements of sections 38(3)-(6) of FIPPA or 28(3)-(6) of MFIPPA and/or best practices
- demonstrating due diligence and evidence of compliance to support informed decision-making during the development of the project (this information may also be important in the event of a privacy breach or complaint to the IPC)
- reassuring individuals, other institutions, partners and your own management that legal requirements and privacy best practices are being followed
- reducing institutional risk by helping to promote more informed and risk-based decision-making and building a culture of privacy within your institution
- improving institutional transparency and enhancing individual awareness, understanding, and trust of your institution's information management practices
- being better prepared in the event of a privacy breach by documenting, in advance, the steps your institution will take to mitigate the risks of a privacy breach, and how it will respond in the event a breach occurs
- improving operational efficiencies, especially when undertaken early and systematically, by helping minimize excessive and unnecessary collection, use, retention and disclosure of personal information, avoiding costly design mistakes and retrofits, and identifying simpler and less costly solutions from the start

Further, PIAs are widely recognized as a best practice in Ontario, across Canada, and globally. They have become essential tools in the analysis of privacy implications associated with information management systems, programs, and technologies used by institutions today.

When to conduct a PIA

Under section 38(3) of FIPPA or 28(3) of MFIPPA, there is a general requirement to conduct PIAs before collecting personal information. Under section 38(5) of FIPPA and 28(5) of MFIPPA, PIAs must also be updated before making any significant change to the purpose for which personal information is used or disclosed.

Institutions should also conduct or update PIAs whenever there are new or changed personal information practices that have the potential to increase adverse impacts on individuals' privacy: for example, changes to technology platforms that house or process personal information, changes to the purposes to which the personal information will be put, or changes to retention periods for personal information.

To be effective, PIAs should be started early in project development or design to build in privacy protection throughout the project's lifecycle — from beginning to end. It is faster, easier and more economical to address privacy risks on a proactive basis during the project design than it is to retrofit privacy protection requirements once your program, process, or system has been implemented.

Responsibility for a PIA

Each institution must decide who will co-ordinate and carry out the PIA. Some institutions will have internal staff who are well-placed to conduct a PIA. Depending on the complexity of the project and the availability of expertise within your institution, you may need to hire an external specialist to conduct your PIA. Institutions also need to define who will review and approve the PIA (separately from who conducted it), who will be responsible for implementing recommendations to address identified privacy risks, and who will be responsible for updating the PIA on an as-needed basis.

In most cases, an effective PIA will require consultation with various individuals who have specialized roles, expertise, and insight into the project.

Methodology

The PIA process generally follows four key steps, each of which is described in detail in this guide.

Step 1: Preliminary analysis

- Examine the project to determine if it will involve the collection, use, retention, disclosure, security or disposal of personal information.
- If you determine that the project WILL involve personal information, proceed with the PIA process. If the project WILL NOT involve personal information, you do not need to proceed with the PIA process.

Step 2: Project analysis

- Gather more specific information about the project, its scope and key characteristics, roles and responsibilities of parties, including third parties, the type of personal information involved and the manner in which the personal information will be collected, used, retained, disclosed, secured or disposed of.

Step 3: Privacy analysis

- Using information gathered in the previous step, identify FIPPA or MFIPPA requirements and potential risks and impacts to privacy.
- Consider ways to reduce or eliminate the risks and impacts identified.
- Assess proposed solutions and their relative advantages and disadvantages.

Step 4: PIA report

- Obtain approval to proceed with recommended solutions.
- Document your findings and chosen solutions in a PIA report.
- Proceed with the project, ensuring that the recommendations from your PIA are fully incorporated in the project plans and implemented.

1. Preliminary analysis

The first step is to determine if the project will involve personal information.[10] If it will not, you do not need to proceed further with the PIA process. Whatever the answer, you should document your conclusion and how you arrived at it. If the project will involve personal information, then you will need to continue with the PIA process.

Helpful resource

Appendix A is a preliminary analysis questionnaire that will help you determine if the project will involve personal information and, if so, identify the types of personal information that will be collected, used, retained, disclosed, secured and disposed of.

What is personal information?

Section 2(1) of both FIPPA and MFIPPA define personal information as ***recorded information about an identifiable individual*** (that is, a natural person). Sections 38(1) of FIPPA and 28(1) of MFIPPA expand the section 2(1) definition to specify that, for the purposes of the collection requirements under FIPPA and MFIPPA[11] personal information includes information that is not recorded. Among other things, this means that the PIA requirements in FIPPA and MFIPPA apply to unrecorded personal information as well as recorded personal information.

Personal information can include, but is not limited to:

- an individual's biographical details (name, sex, age, race)
- an individual's biological details (face, fingerprints, blood type, etc.)
- nationality
- religion
- marital status
- education
- medical or criminal history
- financial information
- identifying numbers, for example, social insurance numbers
- an individual's contact details (personal address, phone number, etc.)
- personal opinions and views

This list of personal information is not exhaustive. An institution may have other types of personal information in its custody or under its control, or additional information that may be considered personal information due to context. There must be a reasonable expectation that an individual can be identified from the information (either alone or when combined with other information) for the information to qualify as personal information.

10 In particular, note that PIAs are required before collecting personal information, subject to any exceptions set out in regulations, as of July 1, 2025 under FIPPA and January 1, 2027 under MFIPPA.

11 Sections 38 and 39 of FIPPA and sections 28 and 29 of MFIPPA.

Tip: Business versus personal information

Information that may seem personal, such as name and contact information, may not be personal information if that information relates to an individual's business activities, that is, they are acting in a professional capacity with respect to that information.

Therefore, it is important to consider the context when determining if the project involves personal information.

Preliminary analysis questionnaire

The preliminary analysis questionnaire (Appendix A) directs you to analyze and document certain aspects of the project and to identify whether it will collect, use, retain, disclose, secure or dispose of personal information and if so, the type of personal information involved.

The questions are designed to be completed by project staff or others without a background in privacy.

You are encouraged to complete the preliminary analysis early in the project so you can determine whether the PIA process and resulting analysis need to be built into the project planning. As a result, it is possible that you may not be able to answer some of the questions. If the answers are unknown when you complete your preliminary analysis, you should revisit it as you proceed with the project and its details become defined.

When completing the preliminary analysis questionnaire, consider all aspects of the project, and think about:

- information recorded in all media (for example, personal information may be stored in paper records, but it may also be stored in electronic media, including emails, video, phone records, computer logs, etc.)
- whether the project involves unrecorded information, for example, information collected orally
- whether previously separate information will be linked (linking information can increase the potential to identify an individual, even if the information itself is not considered personal information)
- whether you will be required to share personal information between programs, institutions or other organizations for the project[12]

12 Information sharing is the disclosure of personal information (including sale) for a specific purpose by the institution that collected the information, to another institution, to another government, to a person or group of persons or to an external organization. Consult your staff responsible for privacy to determine if your institution must comply with information sharing requirements (internal or external). For example, the OPS' Corporate Policy on the Protection of Personal Information defines mandatory requirements for an information sharing agreement.

- whether third parties outside your program area or institution (such as third party service providers) will be able to collect, use, disclose, retain, secure or dispose of any personal information[13]
- whether the project will involve personal information that is maintained for the purpose of creating a publicly available record[14] or excluded from the acts under section 65 of FIPPA and section 52 of MFIPPA (if it does, consult with your legal and privacy staff to determine if you should continue with the PIA process because, for example, other legislation or policies may define privacy requirements that must be complied with)

Once you have completed the preliminary analysis questionnaire, you should have:

- a description of the project's purpose, scope and key objectives
- an understanding of the information involved in the project, and whether or not personal information will be involved
- a description of the types of personal information that will be collected, used, retained, disclosed, secured or disposed of by the project
- a statement about whether you will need to proceed with the PIA, and reasons why or why not

If your analysis determines that the project will collect, use, retain, disclose, secure or dispose of personal information, you should continue with your PIA process. If your preliminary analysis concludes that personal information will not be involved, then a privacy impact assessment will not be necessary, subject to any possible changes over time.

Ensure the project lead and other relevant decision-makers are aware of and agree with your assessment and conclusion. Update the project plan, if required, to make sure all appropriate PIA steps and analyses are completed prior to implementation.

2. Project analysis

If the project will involve the collection, use, retention, disclosure, security or disposal of personal information, you should complete this second step of the PIA process. It extends and deepens the information gathering activities initiated as part of the preliminary analysis (Step 1) and begins to compile information that will be needed to carry out a more detailed privacy analysis (Step 3).

In this step, you will need to define the details of the project so as to identify its potential impact on privacy. Among other things, you will need to identify:

- key characteristics of the project that may create privacy risks
- the activities and business processes involved
- the flow of personal information in the project, including to and from third parties

13 The use of third parties can raise privacy concerns that must be addressed in your PIA. To learn more, refer to the IPC's guidance on ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***.

14 The privacy rules defined in FIPPA and MFIPPA do not apply to personal information that is maintained for the purpose of creating a record that is available to the general public. See section 37 of FIPPA and section 27 of MFIPPA.

- who will be doing what with the information, including, when, how and for what purposes
- the technology or technologies involved in the project

Assemble the PIA team

Identify the subject matter experts needed to complete the project analysis questionnaire (Appendix B), including staff with knowledge in the following areas:

- **Business processes:** relevant business objectives, processes, roles and responsibilities, and required resources
- **Information technology:** relevant technology policies, practices and operational standards
- **Security:** relevant administrative, technical and physical safeguards, practices and measures
- **Information management:** relevant policies, practices, and standards, including applicable retention schedules
- **Legal:** applicable legislation, regulations, bylaws and other legal requirements, service level agreements, memoranda of understanding, contracts, etc.
- **Procurement:** rules and processes, acquired or outsourced product and service solutions
- **Risk assessment:** risk assessment methodology
- **Privacy:** applicable privacy laws, policies, practices, principles and best practices
- **Front end users:** staff and other parties who will use the systems or information collected or created by the project with knowledge and experience with the practical implications

Depending on the scope and complexity of the project, other areas, partners, and interested parties may need to be consulted.

Facilitated group discussions with the various areas impacted by the project may help you complete the PIA steps and better identify and mitigate risks.

Define scope

Define what will be in and out of the scope of your PIA and obtain agreement on the scope from all team members before you begin. Make sure the project lead and other relevant decision-makers approve the scope.

The scope of your PIA may not necessarily coincide with the scope of the broader project. For example, the privacy risks and impacts might arise in only some parts of the project, or your PIA may only need to cover a specific, narrow change to an existing program, process or system and not all aspects of the existing program, process or system.

Assemble relevant background information

Gather all project-related documentation, including information about business processes, workflow, information flows, and business rules. Much of this information may already be found in the project's business case and other project management documentation, previous privacy and security assessments, training materials, policies and procedures and business and IT design documents.

The type of information available will depend on whether you are creating something new or modifying an existing program, process or system and, potentially, the timing of your analysis. Where documentation is incomplete or unavailable, consult with key staff, partners, and other interested parties, including third parties, on existing and proposed activities relevant to the project.

Define relevant business processes

Business processes refer to the various activities that will be conducted during the project. These can include anything from technical processes (such as system back-ups or data processing) to administrative functions (such as reviewing applications, filing and archiving), to policy and ongoing monitoring of a program, system or process. You will need to consult with the subject matter experts in various areas to ensure that you have recorded all applicable activities.

Start by documenting, in a general manner:

- all existing and proposed activities associated with the project (paper based as well as automated), including all parties, technology, and information associated with each activity
- the current information technology environment of your institution, and how it may be impacted by the project
- how the project's business processes will relate to other existing or planned programs, systems or processes, including how information flows from one to another
- whether the project will change an existing program, system or process, and how it will impact or alter current business processes, information flows, roles and responsibilities

Define supporting technology

You should determine if the technology used or developed as part of the project has privacy implications. Identify and document the technology-related components of the project and think about the following:

- How will existing technology be used or new technology be developed to enable or support each step in the business process?
- How will each technology interact with personal information?
- Who will have access to personal information using each technology?
- Are there any back-end processes in these technologies that auto-create records or store information in a way that is not immediately accessible by the user?

Define roles and responsibilities

You should identify and document the roles and responsibilities of all parties to be involved in the project when implemented, noting who may have access to or manage personal information. Make sure to include all relevant partners and other third parties.

If the project will change an existing program, system, or process, determine whether it will change what types of personal information are collected, accessed, used, retained, disclosed, secured, or disposed of. You should also determine how those activities are undertaken, and who is responsible for the personal information throughout the project's lifecycle.

Think beyond dedicated program staff when identifying who will be involved in the business processes and information flows. For example, think about whether the following are or will be involved:

- the public
- clients
- other employees or officers of your institution
- staff in other programs or institutions
- information technology staff (e.g., a system administrator)
- external legal counsel
- other governments
- partners, vendors, or agents of the institution
- consultants
- auditors
- law enforcement agencies

Define relevant information

Consider the various types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of during each business process and activity. In particular:

- identify all records involved (including existing and proposed, hard copy and electronic, etc.)
- describe the types of information that will be collected, accessed, used, retained, disclosed, secured or disposed of in each business process or activity (including recorded and unrecorded information, personal and non-personal information)
- identify any particularly sensitive personal information associated with the business processes, such as medical information, criminal history, etc.

Document personal information flows

Once you have defined the business processes, supporting technology and information, and identified the personal information involved, determine how it will flow through the business processes and technology.

If the project proposes to change an existing program or system, or link different datasets, determine whether it will alter the amount, type, sensitivity or source of personal information involved in the relevant business process.

Map the flow of personal information in all formats, from creation or collection until final disposition (such as, for example, secure destruction or transfer to appropriate archives). Use diagrams or descriptions that are readily understood by the project and decision-makers.

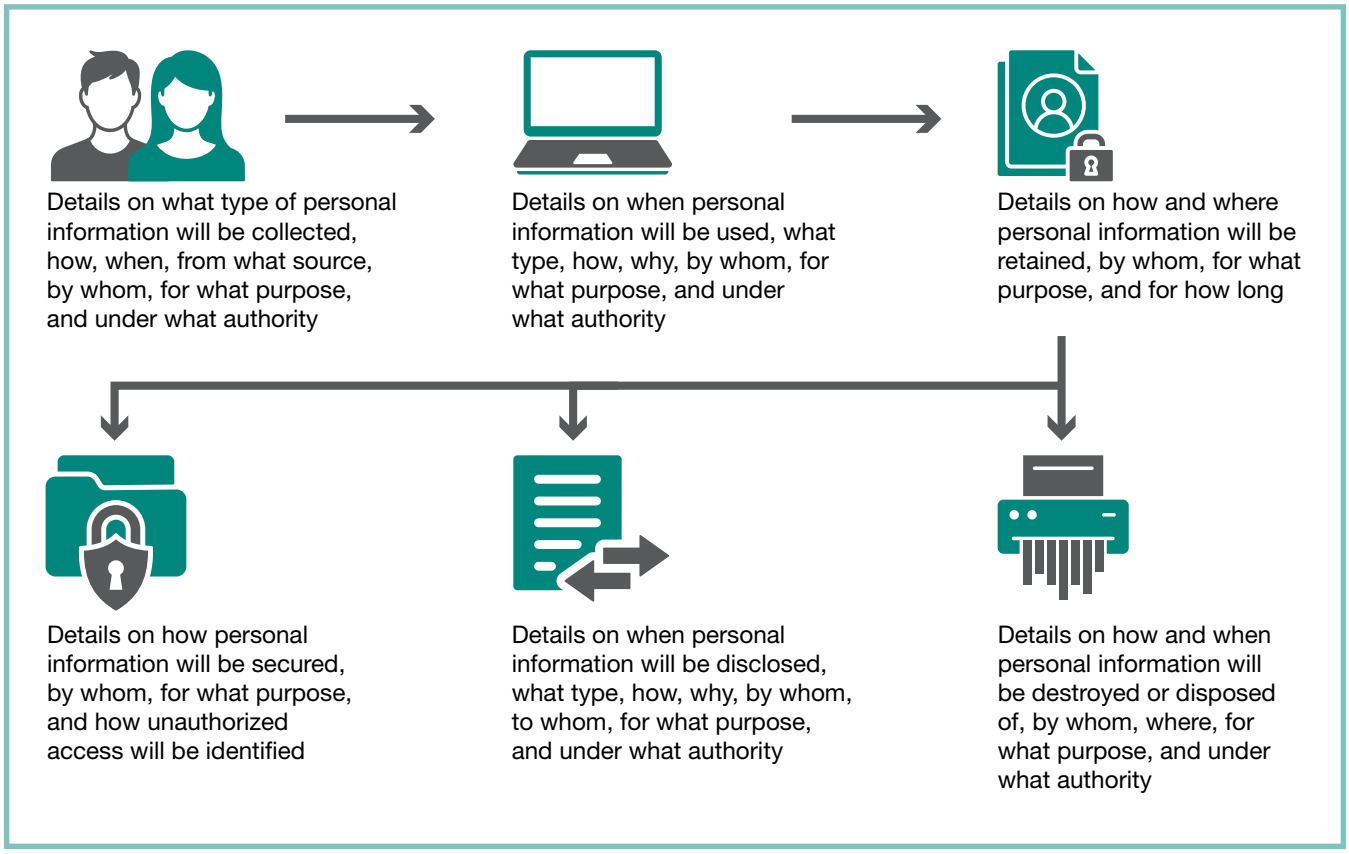
An information flow table or diagram can help you visualize personal information flows associated with the project. These may be organized by some, or all, of the following categories:

- personal information
- source of information
- collected by
- collection method
- purpose of collection
- format of the information
- purpose of use
- used by
- security control during information transfer
- information repository format
- storage retention site
- purpose of disclosure
- disclosed to
- retention policy
- disposal or destruction policy

For example:

Information flow for personal information						
TYPE	COLLECTED	USED	RETAINED	SECURED	DISCLOSED	DISPOSED OF
Details on personal information type	Details on how personal information will be collected, when, where, from what source, by whom, for what purpose, and under what authority	Details on how personal information will be used, when, why, by whom, for what purpose, and under what authority	Details on how and where personal information will be retained, by whom, for what purpose, and for how long	Details on how personal information will be secured, where, by whom, for what purpose, and how unauthorized access will be identified	Details on when personal information will be disclosed, how, when, why, by whom, to whom, for what purpose, and under what authority	Details on how and when personal information will be destroyed or disposed of, by whom, where, for what purpose, and under what authority

Alternatively, information flow diagrams may be visual, such as in this diagram:



3. Privacy analysis

This third step involves a detailed examination of the privacy risks arising from the project and the identification of potential solutions to address them. This will include any mitigation measures, or other limitations or restrictions imposed on the collection, use or disclosure of the personal information.

To be effective, this step should be informed by complete and accurate information about the project, as well as a solid understanding of relevant privacy laws, regulations and other compliance requirements. In addition, your institution's practices related to privacy, information management, technology, security and risk management will also be relevant to your analysis. Existing policies and procedures, or the lack thereof, can be a significant factor in your institution's ability to address privacy risks.

Helpful resource

Appendix C is a privacy analysis checklist that will prompt you to examine your legislative and other privacy requirements and determine and document whether the project will comply. If not, you will need to identify associated privacy risks and impacts and then define action items needed to mitigate them.

Note: Refer to the specific provisions set out in FIPPA or MFIPPA when you are using this checklist to ensure that you have considered all of the provisions of the legislation that may apply to the project.

Privacy impact or risk

A privacy impact is anything that could jeopardize or negatively impact an individual's privacy. For example, theft, loss or unauthorized collection, access, use, retention or disclosure of personal information can result in identity theft or other forms of fraud, physical safety issues such as stalking or harassment, emotional harms such as stress, financial loss, adverse impacts on employment or business opportunities, or damage to reputation.

A privacy impact can also affect your institution. The public can react strongly to a perceived loss of privacy. It can seriously damage your institution's public reputation and result in loss of public trust. It can also cause operational disruptions, affecting the continuity and quality of service. Your institution may also be at legal risk, for example, due to non-compliance with FIPPA or MFIPPA.

Various circumstances can give rise to a privacy impact or risk, such as:

- failure to have the appropriate legal authority to collect, use or disclose personal information
- use of inaccurate, insufficient or out-of-date information

- unnecessary use or disclosure of personal information (for example, where aggregate or de-identified information would instead be sufficient to achieve the purpose or business objective)
- collection, use, or disclosure of irrelevant personal information or of more personal information than what is needed
- retention of personal information for longer than necessary
- failure to keep information appropriately secure
- failure to grant individuals the right to access or correct their own information

Identify potential gaps in compliance

The privacy analysis checklist should be used to identify compliance gaps and the resulting privacy impact or risk. For each question, document your findings in order to conduct an analysis of each identified issue.

The checklist will prompt you to examine whether the project complies with each of the identified privacy requirements. If not, this is a "gap" in privacy protection and an area of potential non-compliance and privacy risk.

These findings should form the basis of your privacy analysis and be documented in the project's PIA report (Step 4).

Consult your information technology and management, security, legal and privacy experts to help you identify and evaluate potential risks and shortfalls in privacy protection.

Tip: Data minimization

Data minimization is the process of limiting the amount of data collected, used, retained or disclosed to only that which is needed to fulfil the purposes of the project. This process includes ensuring the data is destroyed as soon as it is no longer needed. The collection, use, retention or disclosure of unnecessary personal information is an invasion of privacy.

Therefore, as you identify personal information that will be involved in the project, consider carefully if it is necessary to achieve the purpose or business objective.

If not, it should not be collected, used, retained or disclosed. Limiting the amount of personal information you collect, use, retain and disclose will prevent an unnecessary privacy impact.

Analyze findings

Each finding should be analyzed to identify potential privacy risks and impact by considering:

- **Objective:** Start your analysis with the objective of protecting privacy and complying with FIPPA or MFIPPA to maintain public trust.
- **Data minimization principle:** Determine if there is a way to implement the project without collecting, using, retaining or disclosing personal information, or if not, then minimizing the personal information involved.
- **Privacy impact:** Consider the privacy risks or potential impacts resulting from each compliance gap from the perspective of the affected individuals as well as your institution:
  - Try to put yourself in the shoes of the affected individual when assessing harm.
  - Think of the impact on affected individuals, as well as the group(s) of which they are a part.
  - Assess the number of individuals affected, as well as the gravity of the impact. For example, mismanaging the personal information of even a few individuals could have a serious impact on them.
  - Consider the impact on your institution's reputation in the event of non-compliance, and its ability to maintain public trust.
  - Consider the impact on operations, including costs to address a privacy breach after it has happened, when it could have been avoided in the first place.

Understanding the privacy consequences or implications of any compliance gaps is a central part of your privacy analysis. This understanding is necessary to be able to identify action items needed to mitigate the privacy risks and make informed recommendations on how to implement the project in a manner that minimizes any adverse impacts on privacy.

Identify privacy solutions

For each impact, identify actions or possible solutions that will address possible compliance gaps and eliminate or reduce privacy risks. Some common solutions include:

- limiting the amount of personal information involved in the project or deciding not to collect, use or disclose particular types of personal information
- defining or shortening retention periods that will only keep information for as long as necessary and planning for the secure disposal of information
- implementing appropriate administrative, technological, and physical safeguards, practices, and measures
- considering the use of de-identification methods[15] or other privacy enhancing technologies to reduce risks to personal information

15 See the IPC's ***De-identification Guidelines for Structured Data***.

- ensuring that staff are properly trained and aware of the potential privacy impact and appropriate privacy-protective measures to be followed
- producing guidance for staff on how to use new programs, processes, and systems, and how and when it is appropriate to collect, use, access, disclose, and dispose of personal information
- limiting access privileges to only those staff or other individuals or parties who have a need to access personal information for the purpose of carrying out a legitimate business activity
- having staff sign confidentiality agreements on an annual basis to remind them of their obligations to keep personal information secure and of the possible consequences if they do not, in order to discourage lax behaviours or deviation from standard policies, practices, and procedures
- taking steps to ensure that individuals are fully aware of how their information is used and that they can contact the institution for assistance, if necessary (for example, by creating a complete notice of collection and making sure it is accessible to the project's clients)
- selecting third parties that can offer and deliver a greater degree of privacy and security protection, and ensuring that agreements are in place to protect the personal information when in the custody of those third parties
- producing information sharing agreements that clarify what information will be shared, how it will be shared, and with whom it will be shared[16]

Analyze each identified option and consider the potential effectiveness of the solution, and whether it will eliminate or reduce the impact or if it will make the risk acceptable.

Identify action items

Analyzing the effectiveness of each option will help you select the solutions that you believe will be most beneficial for the affected individuals, the project, and your institution. For each impact, identify the specific actions, the responsible party for each item, and the timing for implementation. These will be the mitigation steps needed to minimize privacy risks and potential impacts. Relevant staff should be informed of these and actively involved in implementing mitigation steps as needed.

The action items that you identify are the to do list of items necessary to address prior to project implementation. These will enable the project to achieve its desired objectives while also protecting privacy and complying with FIPPA and MFIPPA.

If the project is already compliant, indicate that no further action is required.

16 An information sharing agreement will clarify the rights and obligations of all parties involved and help with ensuring compliance with FIPPA or MFIPPA. The IPC has guidance on ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***.

4. PIA report

Document the results of your PIA analysis in a way that serves the purpose of the project and supports your decision-makers.

Mandatory information to be contained in a PIA

As of July 1, 2025, under FIPPA and January 1, 2027, under MFIPPA, institutions must have written PIAs that contain, at minimum, the following elements:[17]

- the purpose for collecting, using or disclosing personal information and an explanation of why the personal information is necessary to achieve that purpose
- the legal authority that the institution is relying on to collect, use or disclose the personal information
- the types of personal information to be collected and, for each type, how it is intended to be used or disclosed
- the sources of the personal information to be collected
- the position titles of the institution's officers, employees, consultants or agents who will have access to the personal information
- any limitations or restrictions imposed on the collection, use or disclosure of the personal information
- the period of time that the personal information will be retained by the institution
- an explanation of the administrative, technical and physical safeguards that will be used to protect the personal information and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information
- the steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information and to mitigate risks to individuals

Institutions must provide a copy of their PIA to the IPC upon request.

A written PIA report can help you achieve several important purposes:

- It provides decision-makers with specific recommendations on how to address privacy impacts, and enables them to make informed decisions about how the project should proceed.
- It documents the results of your analysis that may be requested to be seen by the IPC as evidence of your institution's compliance or may be needed for future reference.
- It demonstrates privacy due diligence, and allows you to make a summary of your PIA publicly available to reassure Ontarians and maintain their trust in the project or initiative.

17 See all PIA related requirements in section 38 of FIPPA and section 28 of MFIPPA.

Helpful resource

Appendix D contains a template with instructions for a PIA report. The headings and description of recommended content can help you prepare and format your PIA report. The template should be adapted to meet your project's and institution's needs and legal requirements.

Write your report so it can be readily understood by a non-technical audience (those who are not privacy, legal, technology or security experts). Make sure to include sufficient details and explanations, so that someone outside of the project can understand how you came to your conclusions and recommendations.

Obtain approval

Appropriate approvals of your PIA should be informed by the results of your privacy analysis and your recommended steps to mitigate any privacy risks or impacts.

Approval of your PIA report by the relevant decision maker in your institution should be contingent on:

- a full assessment of the project's privacy risks and impacts
- the decision-makers' understanding of the privacy risks and impacts
- all of the project's identified compliance gaps having been appropriately addressed or accepted
- the decision maker's acceptance of the mitigation steps needed to address the privacy risks and impacts or their acceptance of those privacy risks and potential impacts, should they decide not to proceed with the recommended mitigation steps

Approvals should be properly documented and dated.

Once the action items to address identified privacy risks are approved for implementation, update your PIA report and project plan, if necessary. Institutions must generally implement the steps necessary to prevent and mitigate risks before the collection of personal information can begin.

A copy of your PIA report and all supporting documentation should be included in the project's files to ensure the project team and other key players can access this information, including for the purpose of providing it to the Commissioner upon request.

Update your findings and privacy analysis, as required

As project implementation progresses, continue to assess the project's privacy risks and impacts to determine if you need to update your privacy analysis and PIA report.

Effective July 1, 2025, under FIPPA and January 1, 2027 under MFIPPA, institutions are generally required to update their PIAs and implement any additional prevention and mitigation steps **before** making any significant change to the purpose for which the personal information is used or disclosed.[18] Among other things, updates must include:

- the proposed change to the purpose for which personal information will be used or disclosed and an explanation of why the personal information is necessary to achieve the purpose and
- any additional steps to be taken by the institution to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information and to mitigate risks to individuals in the event of such an occurrence.

This ongoing assessment is an essential part of identifying and mitigating new privacy risks and impacts that arise during implementation.

As the project is implemented:

- monitor progress of privacy-related activities to make sure they are appropriately completed
- assess any changes to the project's implementation (such as business process, information flows, roles and responsibilities) to ensure that new privacy risks have not been created by these changes
- evaluate risk prevention and mitigation steps to determine if they are effective when implemented, and update or revise them if necessary
- identify and assess new, outstanding and remaining privacy gaps and impacts, and identify new action items required to address them
- alert the project lead and relevant decision-makers to any new privacy-related problems, and obtain appropriate approvals to address or accept the privacy risks
- update or supplement your PIA documentation, as required, ensuring you document:
    - the new privacy risks and impacts and how they arose
    - their likelihood, harm and priority for action
    - your mitigation steps to address the new privacy risks

The project lead and other appropriate decision makers should approve all significant changes impacting privacy and the acceptance of any privacy risks, and all such approvals should be documented.

18 See sections 38(3)-(5) of FIPPA and sections 28(3)-(5) of MFIPPA.

Tip: Monitoring and re-assessing

Ensuring the project protects privacy and complies with applicable privacy legislation is not a one-time activity. New issues and changes impacting privacy and compliance may also develop post project implementation.

Therefore, the party or parties responsible for privacy protection and compliance should, on an on-going basis, monitor developments or changes to key aspects of the project. For example, this may involve changes to the purpose for which personal information is used or disclosed, the project scope, business owner, legislative or regulatory authority, business processes, partners or third party service providers, technology functionality, service delivery model, security and information requirements. Such changes may create new privacy risks and trigger the need to update your privacy analysis and prevention and mitigation steps.

When changes or developments occur that impact the project, your institution may need to revisit your PIA and either change it or add to it. Your institution may decide to amend your original PIA or prepare and addendum to your original PIA report. Either way, any changes should be duly documented.

Concluding the PIA process

Before you conclude your PIA process:

- make sure all privacy-related decisions, analysis and actions are appropriately documented
- transfer your PIA documentation to the appropriate parties, such as the program area, or provide them with a copy, to enable ongoing privacy protection and the management of privacy risks once the program, process or system becomes operational

As of July 1, 2025, under FIPPA and January 1, 2027 under MFIPPA, institutions are required to provide a copy of their PIA report to the IPC upon request.[19]

19 See section 38(6) of FIPPA and 28(6) of MFIPPA.

Appendix A: Preliminary analysis questionnaire

1. Project and institution

PROJECT TITLE	
INSTITUTION	
DEPARTMENT	
PROJECT LEAD	

2. PIA lead

NAME AND TITLE	
INSTITUTION	
DEPARTMENT	
PHONE NUMBER	
E-MAIL	

3. Project description

Describe the project (for example, the program, system, application or activity) that is the subject of the PIA, including its purpose, scope, and key objectives. Attach relevant project documentation, if necessary.

4. Collection, use, and disclosure

4.1 Identify the kinds of information involved in the project (check all that apply).

	YES	NO	UNKNOWN
Information about individuals in their personal capacity			
Information about individuals acting in their business, professional or official capacity (for example: name, job title, and business contact information)			
Information about institutions (for example: for profit and not-for-profit institutions and government institutions)			
Aggregated or de-identified information. In the row below, outline the process followed to aggregate or de-identify the information and the potential to identify/ re-identify individuals from that information.			

4.2 Identify the kinds of personal information that will be collected, used, retained, disclosed, secured and disposed of (check all that apply).

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
No personal information						
Unknown at this time (please explain why in row below).						

	COLLECT	USE	RETAIN	DISCLOSE	SECURE	DISPOSE
In the rows below, list the types of personal information involved in the project (add more rows as needed). If third parties will be involved in the project, think about what they may be doing with personal information as well.						
In the rows below, list each element of non-personal information that, when combined or linked, may enable identification of an individual (add rows as necessary).						

4.3 To whom does the personal information relate? List the individuals whose personal information will be involved in the project (in other words, the data subjects).

5. Privacy legislation

5.1 Identify applicable privacy legislation (check all that apply).[20]

	YES	NO	UNKNOWN
Freedom of Information and Protection of Privacy Act			
Municipal Freedom of Information and Protection of Privacy Act			
None or other (Please explain below.)			

5.2 Public records and excluded personal information[21]

	YES	NO	UNKNOWN
Does the project involve any personal information that will be maintained for the purpose of creating a record that is available to the general public? What is the type of personal information, and why and how is it made available to the general public? Please explain in the row below.			
Does the project involve any personal information that will be excluded from the application of the acts by section 65 of FIPPA and section 52 of MFIPPA? What is the type of personal information, and why is it excluded? Please explain in row below.			

20 See the ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*** for information about conducting a PIA involving personal health information regulated under that act.

21 Consult with your legal and privacy staff to determine if you should continue with the PIA process, and if other legislation or policies define privacy requirements that must be complied with.

6. Conclusion

Indicate whether you will proceed with the PIA process and the reasons for your decision. (Institutions must complete a written PIA before collecting personal information, unless a regulatory exception applies.)

Appendix B: Project analysis questionnaire

1. Scope of PIA

Define the scope of the PIA review and analysis. What aspects of the project are in and out of scope?

2. Project authority

Describe the regulatory and legal framework for the project (for example, applicable legislation and regulations, bylaws, memoranda of understanding, agreements, contracts and other relevant instruments).

3. Project characteristics

3.1 Identify key characteristics of the project (check all that apply).

DOES THE PROJECT INVOLVE...	YES	NO	UNKNOWN
creating a new program, process, service, technology, information system or other type of IT application?			
a change to an existing program, process, service, technology, information system or other type of IT application?			
a new collection of personal information?			
procuring goods or services?			
outsourcing or contracting for services related to the collection, use, disclosure, processing, retention, storage, security or disposal of personal information?			
developing a request for bids, proposals, or services?			
a process, system or technology for which the privacy risks are not known or well documented?			
creating an information system or database containing personal information, and/or the matching, merging, combining or centralizing of databases?			
information sharing (internal and external)?			
the need to identify, authenticate or authorize users – including public and/or internal staff?			
other activities that may impact privacy? (Please explain below.)			

3.2 If you answered yes to any of the above, explain the identified process or activity. Attach all relevant documentation to your completed project analysis questionnaire.

3.3 Identify any changes that will result from the project (check all that apply).

WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change in business owner?			
a change to legislative authority?			
a change in users (internal and external) of a related process or system?			
a change in partners or service providers (internal and external)?			
a change in the amount, type of, or ways that personal information is collected, used, disclosed, retained, secured or disposed of?			
a change to the purposes for which personal information will be collected, used, or disclosed?			
a change from direct to indirect collection of personal information?			
a change in roles and responsibilities (such as who can do what, when, where, why and how with personal information)?			
a change to, or elimination of, existing practices of de-identifying information?			
a change in the process or technology used to collect, use, disclose, retain, secure or dispose of personal information (for example: hardware and software)?			
a change to an information system or database containing personal information?			

WILL THE PROJECT INVOLVE...	YES	NO	UNKNOWN
a change of medium or service delivery channels (for example: the automation of manual processes, conversion from paper to electronic records, or the creation of a new website to provide services to clients)?			
a change in the security requirements or safeguards, practices, or measures?			
other changes (please specify change or proposed change below)?			

3.4 If you answered yes to any of the above, explain the change(s), including what specifically will change and why it is necessary. Attach all relevant documentation to your completed project analysis questionnaire.

3.5 Document any additional business processes identified from your analysis of the factors identified in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

4. Technology

4.1 Identify technology-related characteristics of the project (check all that apply).

DOES THE PROJECT INVOLVE...	YES	NO	UNKNOWN
technology designed to monitor, track or observe an individual or their transactions (for example: video cameras, cell phones, and geospatial or location-based services)?			
logging information, usage or preferences (for example: IP addresses, traffic data, access or transaction logs, cookies, or other mechanisms for recording an individual's use of technology)?			
public-facing Internet communications, services or transactions, including websites, blogs, forums, bulletin boards, or social media?			
using analytics or performance measurements (for example: web analytics, social media analytics, or business intelligence tools)?			
processing or storing of personal information in a virtual environment (for example, cloud computing)?			
acquiring or customizing commercial software, hardware, or IT support services by external vendors?			
developing or customizing software, hardware, or IT support services in-house?			
creating information systems or other types of IT applications that will be populated by others (for example, clients of a system or service will supply information)?			
a system or application that will automatically collect, use, disclose or retain personal information?			
other (Please explain below.)			

4.2 If you answered yes to any of the above, provide an explanation of the technology (that is, purposes, why necessary, and how used). Include your answers to the technology questions in the guide. Attach all relevant documentation to your completed project analysis questionnaire.

5. Roles and responsibilities

5.1 List other institutions or other third parties involved in developing or implementing the project and describe their role.

INSTITUTION/THIRD PARTY	PROJECT ROLE

5.2 List all institutions or other third parties that will collect, use/process, retain, store, disclose, secure, or dispose of personal information <u>on behalf</u> of your institution.

INSTITUTION/ THIRD PARTY	RELATIONSHIP TO INSTITUTION	PROJECT ROLE

5.3 Identify any location outside of Ontario where personal information may be retained or stored and the third parties involved.

PERSONAL INFORMATION	LOCATION	THIRD PARTY

5.4 List all position titles of the officers, employees, consultants, or agents of your institution who will have access to the personal information. For example, program area staff (by title), IT staff, legal counsel, etc.

POSITION TITLE	RELATIONSHIP TO PROJECT	PROJECT ROLE

5.5 Identify how other institutions or third parties will be bound to follow relevant privacy and security requirements (check all that apply).

	NAME OF INSTITUTION OR THIRD PARTY	IN PLACE	BEING DEVELOPED	UNKNOWN
contracts				
memoranda of understanding				
agreements (service level and trade)				
other (Please explain below.)				

6. Relevant information

Document what and how all types of information relate to each business process and activity relevant to the project. Consider the factors identified in the guide. Attach all related documentation to your completed project analysis questionnaire.

7. Personal information flows

Document, in detail, the lifecycle of the personal information involved in the project in a manner that suits the project's and your institution's needs. This can be done by an information flow table or diagram. Specify the personal information involved in the project from creation and collection to final disposition. Attach any documentation needed to support your identified flows of personal information throughout the project to your completed project analysis questionnaire.

Appendix C: Privacy analysis checklist

Answering the following questions can help you to identify the privacy risks that need to be addressed and the steps to be taken to ensure compliance with FIPPA or MFIPPA. You can use the table below to organize your work, or it can be adapted to meet the needs of the project and your institution. Be sure to address all the identified questions and consider each instance of how personal information is involved when completing the checklist. For example, when asked about authority to collect, consider all the types of personal information you will collect.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y[22]	N[23]	IP[24]	NA[25]	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
Review each question and determine how each relates to the project. **Note:** Do not use the checklist as a substitute for the legislation. The statutory provisions have been summarized here.	Put a check mark (√) in the appropriate column for each question. This will create a visual representation of the project to assist with complying with FIPPA or MFIPPA. If your findings differ depending upon the type of personal information involved, add rows to document and explain the differences for each type.				Outline how you arrived at your findings. Provide as much information as is available, particularly if action is planned, but not yet implemented. Outline any options or alternatives that were, or need to be, considered. Explain why no action has been taken or planned for each "N" finding, and why requirements are "NA" to the project.	For each finding, outline the potential impact or risk to privacy. For example: a theft, loss or unauthorized use or disclosure of the personal information, non-compliance with FIPPA or MFIPPA, increased intrusiveness into the private lives of individuals, or it does not meet the public's expectation of privacy.	For each finding, identify the action(s) (steps) necessary for compliance with the privacy requirement or to mitigate or prevent a potential privacy impact or risk.

22 **Y (Yes):** You know the privacy protection requirement either has been met by existing safeguards, practices or measures or will be met by action planned before implementation

23 **N (No):** You know nothing has been done or is planned to address this privacy protection requirement; there is a possible privacy risk and "gap" in the project's compliance. If nothing has been done or planned, explain why.

24 **IP (In Progress):** You do not know the answer to the question at this time; more information or analysis is required and, until such time, there is a potential privacy risk and gap.

25 **NA (Not Applicable):** You know this privacy protection requirement is not applicable to the project. Note: Be sure to check with your FIPPA or MFIPPA Coordinator and Legal Counsel.

A. Collection

Key requirements:

- A written PIA report must be prepared before collecting personal information.
- For each collection of personal information, ensure that the institution collects personal information only if it has the authority to do so. Consider the following:
  - Is the collection expressly authorized by statute?
  - Will the personal information be used for law enforcement purposes?
  - Is the collection necessary for the proper administration of a lawfully authorized activity?
  - Why is personal information necessary to achieve the purpose of the collection?
- Personal information must be collected directly from the individual to whom it relates, unless another manner of collection is authorized by the individual or other statutory provision.
- Notify the individual of the collection, including legal authority, purpose(s), and contact information of a person who can answer questions about the collection.
- Risk prevention and mitigation steps must generally be implemented by the institution before collecting personal information.
- See sections 28 and 29 of MFIPPA and sections 38 and 39 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Is the collection of personal information authorized under FIPPA or MFIPPA or another act?							
Do all parties collecting personal information have legal authority for the collection?							
Have you documented the legal authority for the intended collection?							
Has responsibility for the collection been assigned to program staff or third party service providers?							
PURPOSE OF COLLECTION							
Has each purpose of the collection been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
NOTICE TO INDIVIDUAL							
Will notice of collection be provided to the individual(s)? Explain timing, method, and exemptions from notice, where authorized.							
Will the notice of collection comply with FIPPA or MFIPPA? Explain how or if there are missing components.							
MANNER OF COLLECTION/SOURCE OF PERSONAL INFORMATION							
Will personal information be collected directly from the individual? Explain the types, sources and form of collection.							
Will personal information be collected indirectly from another source, or covertly? Why?							
Will indirect collection comply with FIPPA or MFIPPA? Explain the authority for indirect collection.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will the project only collect personal information for which there is legal authority?							
Will there be any limitations or restrictions imposed on the collection of the personal information?							
Will there be periodic reviews of the collection controls to ensure effectiveness?							
DATA MINIMIZATION							
Is personal information necessary for the project to proceed?							
Is collection of all the personal information necessary? Why or why not?							

B. Use

Key requirements:

- For each use of personal information, ensure that all parties involved in the project, including your institution, partners and other third parties, use personal information only with the authority to do so. Consider the following:
  - Is the use for the purpose it was collected or for a consistent purpose?[26]
  - Is the use authorized by the individual to whom it relates?
  - Does the use comply with another statute?
  - Is the use for other purposes permitted by FIPPA or MFIPPA?
  - Why is personal information necessary to achieve the purpose of the use?
- Before making any significant change to a purpose for which personal information is used, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 31 of MFIPPA and sections 38 and 41 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Do all parties using personal information have the legal authority for the use(s)?							
Have you documented the legal authority for the intended use(s)?							

26 A consistent purpose is a use of personal information that the individual to whom the personal information relates might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
PURPOSE(S) OF USE							
Has each purpose of use been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be used for other purposes?							
Will uses of personal information be for purposes stated in the notice of collection or for a consistent purpose?							
MANNER OF USE							
Have all parties using personal information been defined by position title (for example: program staff, consultants, agents of the institution, third party service providers, employees, officers etc.)?							
Have you indicated how each type of personal information will be used?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will there be administrative, technical, and physical safeguards, practices, and measures in place to ensure personal information will be used only for authorized purposes and by authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the use(s) of the personal information?							
Will there be periodic reviews of the use safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is use of all the personal information necessary for the project to proceed? Why or why not?							

C. Disclosure

Key requirements:

- For each disclosure of personal information, ensure that all parties involved in the project disclose personal information only with the authority to do so. Consider the following:
  - Is the disclosure for the purpose for which it was collected or for a consistent purpose?[27]
  - Is the disclosure authorized by the individual to whom the personal information relates?
  - Does the disclosure comply with another statute?
  - Is the disclosure for other purposes permitted by FIPPA or MFIPPA?
  - Why is the personal information necessary to achieve the purpose of the disclosure?
- Before making any significant change to a purpose for which personal information is disclosed, update the PIA report to, among other things, reflect the proposed change and implement additional risk prevention and mitigation steps.
- See sections 28 and 32 of MFIPPA and sections 38 and 42 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
AUTHORITY							
Do all parties disclosing personal information have the legal authority for the disclosures?							
Have you documented the legal authority for the intended disclosures?							

27 A consistent purpose is a disclosure of personal information that the individual to whom the personal information relates, that is, the data subject, might reasonably expect at the time of collection.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
PURPOSE(S) OF DISCLOSURE							
Has each purpose of disclosure been defined, including why personal information is necessary to achieve the purpose? Explain the purpose(s).							
Will personal information be disclosed for other purposes?							
Will disclosures of personal information be for purposes stated in the notice of collection or for a consistent purpose?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MANNER OF DISCLOSURE							
Have all parties disclosing personal information been defined (for example: program staff, consultants, agents, third party service providers, employees, officers, etc.)?							
Have you indicated how each type of personal information will be disclosed?							
Has the manner of disclosure been defined (for example: oral, mail, email, etc.)?							
Will the disclosures be documented and how?							
INFORMATION SHARING AGREEMENT							
Will disclosures be documented and controlled by information sharing agreements or other means?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will there be administrative, technical and physical safeguards, practices and measures in place to ensure personal information will be disclosed for authorized purposes, by and to authorized parties? Explain the safeguards, practices and measures.							
Will there be any limitations or restrictions imposed on the disclosures of the personal information?							
Will there be periodic reviews of the disclosure safeguards, practices and measures to ensure effectiveness?							
DATA MINIMIZATION							
Is disclosure of all the personal information necessary for the project to proceed?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
DISCLOSURE FOR RESEARCH PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for research purposes?[28]							
DISCLOSURE FOR FUNDRAISING PURPOSES							
Is it reasonably likely that personal information will need to be disclosed for fundraising purposes?[29]							

28 Before such a disclosure, there should be a defined and documented process that makes sure the researcher demonstrates why identifiable information is required for the research purpose. The researcher must agree to the terms and conditions of Ontario Regulations 460 and 823, section 10.

29 FIPPA defines when disclosure of personal information by educational institutions or hospitals may be done for fundraising purposes. Before such disclosures, ensure the requirements, as defined in sections 42(2) and (3), have been met.

D. Accuracy and correction

Key requirements:

- Take reasonable steps to ensure personal information is not used or disclosed unless it is accurate, complete and up to date.
- Ensure that every individual can:
  - correct their personal information
  - have a statement of disagreement attached to the personal information if the correction is not made
  - require a notice of the correction or the statement of disagreement to be sent to anyone to whom the personal information was disclosed within the year before the above action was taken
- See sections 30(2) and 36 of MFIPPA and 40(2) and 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
STANDARD OF ACCURACY							
Will there be steps in place to make sure personal information is not used, unless it is accurate, complete and up-to-date? Provide details of the steps.							
CORRECTING THE PERSONAL INFORMATION							
Will there be a defined and documented process for the processing of a request for the correction of personal information? Provide details of the process.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CORRECTION REQUESTS/STATEMENT OF DISAGREEMENT							
Will there be a defined and documented process for individuals to request the correction of their personal information? Provide details of the process.							
CONTROLS							
Will controls be in place to ensure that only authorized personnel will be able to add, change, or delete personal information?							
Will there be periodic reviews of the controls to ensure effectiveness?							

E. Security

Key requirements:

- Take all reasonable measures to prevent unauthorized access to personal information in your custody or control, taking into account the nature of the record to be protected.
- Access should be restricted to only those individuals who need the personal information for the performance of their duties.
- Explain the safeguards, practices and measures that will be used to protect the personal information.
- Summarize any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of personal information
- Take all reasonable safeguards, practices and measures to protect personal information against loss or theft, unauthorized access, use or disclosure, inadvertent modification, destruction or damage, taking into account the format of the record to be protected.
- See Ontario Regulation 823, section 3 as well as sections 28 and 30(5) of MFIPPA, and Ontario Regulation 460, sections 3 and 4, as well as sections 38 and 40(5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
SECURITY MEASURES							
Will safeguards, practices and measures be used to protect the personal information? Explain each administrative, technical and physical safeguard, practice and measure.							
Will risk prevention and mitigation steps be implemented before collecting the personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will security safeguards, practices and measures be defined and documented to protect the confidentiality, integrity and availability of personal information?							
Will testing and periodic reviews be conducted to ensure that personal information is only collected, accessed, used, disclosed, retained and disposed of when authorized and is not stolen or lost?							
Will all actions relating to the collection, use, disclosure, retention, correction, copying or disposal be logged and subject to auditing and monitoring?							
Will procedures be defined and documented on how to identify, report, investigate and address the theft, loss and/or unauthorized access, collection, uses and/or disclosure of personal information?							

F. Requesting access to personal information

Key requirements:

- Ensure that every individual has a right of access to their personal information in the institution's custody or control.
- Make sure that personal information in the institution's custody or control is retrievable.
- Verify the identity of persons requesting access to their personal information.
- See section 36 of MFIPPA and section 47 of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
ACCESS REQUESTS							
Will the management of personal information change or restrict individuals' right of access to their personal information?							

G. Retention

Key requirements:

- Personal information should be retained for at least one year after use to provide the individual with a reasonable opportunity to access their personal information.
- The individual's consent should be obtained in order to dispose of personal information prior to one year after use.
- Ensure compliance with other relevant records retention laws, regulations, bylaws or other requirements.
- See MFIPPA sections 28(3), 30(1), 30.1(8) and Ontario Regulation 823, section 5; FIPPA sections 38(3), 40(1), 40.1(8) and Ontario Regulation 460, section 5.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
RETENTION SCHEDULES							
Will there be defined and documented policies, procedures, and other requirements related to the retention of personal information?							
REASONABLE OPPORTUNITY FOR ACCESS							
Will safeguards, practices and measures be in place to ensure that personal information will be retained for a minimum of one year after its last use?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MEDIUM AND LOCATION OF RETENTION							
Has the medium and format of the personal information to be retained been defined?							
RETENTION PERIOD							
If the personal information has not been used, will it be retained for only as long as necessary to meet its purpose? How long will it be retained?							
How long will personal information that has been used be retained?							
CONTROLS							
Will procedures be defined and documented related to consent for early disposal of personal information?							
Will there be periodic reviews of the retention requirements and consent procedures to ensure effectiveness?							

H. Disposal and destruction

Key requirements:

- Personal information must be disposed by either securely destroying it or transferring it to the appropriate archives.
- Make sure personal information is only destroyed when authorized by an appropriate party and in accordance with records retention laws/regulations/bylaws applicable to the institution.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be destroyed throughout the process, that is, when personal information is stored, transported, handled and destroyed.
- Take all reasonable safeguards, practices and measures to protect the security and confidentiality of personal information to be transported to archives throughout the process, that is, when personal information is stored, transported and handled.
- Take all reasonable safeguards, practices and measures to destroy personal information so it cannot be reconstructed or retrieved.
- Keep an accurate record of the disposal, including what personal information was destroyed or transferred and on what date it was destroyed or transferred.
- Do not include personal information in your record of disposal.
- See Ontario Regulation 823 and section 30(4) and (5) of MFIPPA, and Ontario Regulation 459 and sections 40(4) and (5) of FIPPA.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
MANNER OF DISPOSAL							
Will procedures be defined and documented for the secure disposal, for example, transfer to archives or destruction of personal information in accordance with applicable records retention schedules, laws/ regulations/ bylaws? Explain the disposal process.							
DEVICES/EQUIPMENT							
Will procedures be defined and documented for disposal of devices and equipment containing personal information?							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
CONTROLS							
Will safeguards, practices and measures be defined and documented to ensure only appropriate personal information will be disposed of or destroyed, and only by authorized parties after obtaining appropriate approval?							
Will there be periodic reviews of the disposal safeguards, practices and measures to ensure effectiveness?							
RECORD-KEEPING							
Will details of the disposal of personal information be recorded?							
Will safeguards, practices and measures be defined and documented to ensure no personal information is captured in the disposition record?							

I. Privacy management

The questions in this section relate to privacy management throughout your institution. They are not limited to the project's information system, technology, or program, but address your institution's privacy maturity, capability, and readiness to undertake the project. The emphasis is on accountability and training.

Key requirements:

- Apply common management principles, such as planning, directing, controlling and evaluating the personal information collected, used, disclosed, retained and destroyed by institutions.
- Establish and follow disciplined and consistent practices for the management of personal information.
- Educate staff about privacy, as well as legislative and other relevant requirements.
- Periodically review safeguards, practices, and measures, and commit to ongoing improvement in compliance.

PRIVACY REQUIREMENT QUESTIONS	FINDINGS					PRIVACY IMPACT/RISK	ACTION ITEMS
	Y	N	IP	NA	EXPLANATION		
ACCOUNTABILITY							
Will accountability for managing personal information throughout its lifecycle be defined to include parties involved in the project(for example: your institution, **officers, employees, consultants or agents of your institutions**, partners, vendors and other third parties)? Explain accountability.							

PRIVACY REQUIREMENT QUESTIONS	FINDINGS Y	N	IP	NA	EXPLANATION	PRIVACY IMPACT/RISK	ACTION ITEMS
TRAINING							
Will operational safeguards, practices, and measures related to the protection of personal information be needed?							
Have all parties requiring training on operational, security, and privacy aspects of the project been identified?							
Has the individual responsible for ensuring that all parties receive appropriate training been identified?							
AUDITS							
Will safeguards, practices, and measures be developed and documented to evaluate whether the personal information is accessed, collected, used, retained, disclosed, secured, and disposed of in a manner that is consistent with FIPPA or MFIPPA, or if it is stolen or lost?							

Appendix D: PIA report template

Mandatory information to be contained in a PIA

As of July 1, 2025, under FIPPA and January 1, 2027, under MFIPPA, PIAs are mandatory before collecting personal information (subject to any prescribed exceptions) and must contain, at minimum, the information set out in section 38 of FIPPA or section 28 of MFIPPA:

1. The purpose for which the personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose.
2. The legal authority for the intended collection, use and disclosure of the personal information.
3. The types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed.
4. The sources of the personal information that is intended to be collected.
5. The position titles of the officers, employees, consultants, or agents of the institution who will have access to the personal information.
6. Any limitations or restrictions imposed on the collection, use, or disclosure of the personal information.
7. The period of time that the personal information would be retained by the institution, in accordance with subsection 40(1) of FIPPA or 30(1) of MFIPPA.
8. An explanation of the administrative, technical and physical safeguards, practices and measures that would be used to protect the personal information in accordance with subsection 40(5) of FIPPA or 30(5) of MFIPPA and a summary of any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.
9. The steps to be taken by the institution,
    i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    ii. to mitigate the risks to individuals in the event of such an occurrence.
10. Such other information as may be prescribed.

Risk prevention and mitigation steps outlined in the PIA must generally be implemented before collecting personal information. It is important that you review both new and existing legal requirements when preparing your PIA report and ensure that it includes all required information.[30]

30 See PIA requirements in section 38 of FIPPA and section 28 of MFIPPA..

Provincial and municipal institutions should use this PIA report template as a best practice document but not as a substitute for the legislation. You should consult with your legal and privacy staff if you have questions about completing a PIA and ensuring compliance with FIPPA or MFIPPA.

Title page

Include the project name, institution/department, date, and the identity of the party who completed the PIA process and prepared the PIA report.

Executive summary

- Provide reviewers and decision-makers with an overview of the project.
- Summarize your key findings, recommendations, and action items.
- Note any outstanding privacy impact.

Table of contents

Include main headings, subheadings, and appendices to enable reviewers to readily locate information.

Introduction

Explain:

- the objective of the project
- the purpose of the PIA Report and the attached appendices
- the response being sought and timelines

Background

General

Provide high-level context for your analysis and findings, including, but not limited to:

- **PIA:** Briefly describe the PIA process including the purposes and outcomes of the preliminary analysis, project analysis, and privacy analysis. Attach completed questionnaires and checklists and supporting documents.
- **Scope:** Briefly describe what is in-scope and out-of-scope in your PIA. Note any related projects, programs, or systems, relevant PIA work, or other risk analysis undertaken by other parties.
- **Glossary:** Explain specialized terms and acronyms used in your PIA analysis and documentation.

Project

Provide a summary of the project including as much detail as is necessary to enable reviewers and decision-makers to understand the project in the context of your privacy analysis. Include the following, in addition to any specific information that you believe is necessary:

- description of the project
- accountability for the project
- related initiatives and linkages
- project partners and interested parties

Privacy

Provide context for your analysis of the project's impact on privacy, including, but not limited to:

- **Personal information:**

  Describe the:

  - purposes for which personal information is intended to be collected, used, and disclosed, as applicable, and an explanation of why the personal information is necessary to achieve the purpose
  - types of personal information that is intended to be collected and, for each type of personal information collected, an indication of how the type of personal information is intended to be used or disclosed
  - source(s) of personal information to be collected, including the category(ies) or class(es) of individuals represented in those sources

  Among other things, note whether the project will have a broad impact, involve significant amounts of personal information about any individuals, or involve sensitive information.

- **Legal authority:** Identify the legal authority for the project and for collecting, using, and disclosing personal information. Include references to:
  - enabling legislation for the project
  - applicable privacy legislation, for example, FIPPA or MFIPPA
  - related agreements with partners, agents, and other third parties
- **Privacy roles and responsibilities:** Identify the individuals and parties (internal and external to your institution) responsible for protecting privacy. Explain their roles and responsibilities.

- **Access roles and responsibilities:** Identify the position titles of those who will have access to the personal information, including all officers, employees, consultants or agents of the institution.
- **Limitations:** Identify any limitations or restrictions imposed on the collection, use or disclosure of personal information.
- **Retention period:** Explain the period of time that the personal information would be retained by the institution.
- **Interested parties:** Identify relevant partners and interested parties and their importance to your privacy analysis. Indicate any conducted or planned consultation, the purpose, and the results.
- **Administrative, technical, and physical safeguards, practices, and measures:** Explain all safeguards and practices that would be used to protect personal information from theft, loss or unauthorized use or disclosure.
- **Risks to individuals:** Identify and summarize any risks to individuals in the event of a theft, loss, or unauthorized use or disclosure of the personal information.

Business processes and information flows

You should explain relevant businesses processes, both existing and planned, including:

- changes to existing processes
- the key roles and responsibilities
- the use of technology related to those business processes

Identify who does what, as well as why, when, where, and how they do it.

Describe how personal information will flow through the business processes and technology. Describe how personal information will be collected, used, retained, disclosed, secured, and disposed of, including changes to:

- existing information flows
- amounts or types of personal information involved
- who will have access to the personal information and be responsible for it throughout its lifecycle

Use plain language and organize this information in a way that makes sense for the project. For example, a complex project may require a broad overview as well as more detailed descriptions of its component parts.

Privacy analysis

Explain the results of your completed privacy analysis, including:

- your findings
- the privacy impact and risk(s) related to each finding
- your recommendations on what needs to be done to protect privacy and comply with FIPPA or MFIPPA
- your risk prevention and mitigation steps to:
    - prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and
    - mitigate the risks to individuals in the event of such an occurrence
- priorities and proposed timelines and responsibility for implementation

From this section, the reviewers and decision-makers should have a clear understanding of:

- the legal authority for the project (legislative and other instruments)
- the project's privacy risks
- the work that needs to be undertaken by the institution to protect privacy to comply with applicable privacy legislation
- outstanding, remaining, or unmitigated privacy risks and other issues impacting privacy and how they will be addressed

Conclusions

Include any final remarks relevant to your PIA. For example, indicate whether the purpose of your analysis was successfully achieved or if outstanding privacy work must be completed, etc.

Note key characteristics of the project including, but not limited to, whether it:

- could enhance privacy protection and compliance with privacy requirements
- could be designed to avoid, eliminate, or reduce some or all of the identified privacy risks
- could result in an unjustified invasion of privacy
- will involve new technology, business rules, or processes for which the privacy risks are not known or well documented

Next steps

Highlight any required follow-up to your privacy analysis, such as the timing and priorities for implementing your risk prevention and mitigation steps, or requirements to update the PIA in the future.

Determine and document where your organization will maintain the final approved PIA report. Ensure that this location is known and accessible within the institution (for example, in a centralized PIA repository maintained by the privacy office), so that it may be easily retrieved for review, updating, and providing to the IPC if required.

Approval

The project lead and other relevant decision-makers should approve the PIA report and acknowledge, in writing, that they understand the findings and recommendations, and authorize implementation of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks. This includes documenting in the PIA report the steps to be taken:

i. to prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring, and

ii. to mitigate the risks to individuals in the event of such an occurrence.

Attachments

Attach relevant documentation to support the findings and recommendations in this report. Examples of possible attachments include, but are not limited to:

- explanation of FIPPA and MFIPPA provisions (e.g., custody and control)
- list of documents reviewed and interviews conducted
- copies of cited forms
- completed PIA documents, including:
    - preliminary analysis
    - project analysis
        - business process diagrams
        - roles and responsibilities chart
        - information flow diagrams
    - privacy analysis checklist
- summary of recommendations and action items

Appendix E: Additional resources

Ontario privacy legislation, regulations, and other guidance

The *Freedom of Information and Protection of Privacy Act* (FIPPA)

- ***The Freedom of Information and Protection of Privacy Act***
- **Disposal of Personal Information – R.R.O. 1990, Reg. 459**
- **General – R.R.O. 1990, Reg. 460**

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA)

- ***The Municipal Freedom of Information and Protection of Privacy Act***
- **General – R.R.O. 1990, Reg. 823**
- **Institutions – R.R.O. Reg. 372/91**

Other IPC guidance

- ***Privacy and Access in Public Sector Contracting with Third Party Service Providers***
- ***De-identification Guidelines for Structured Data***
- ***Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act***

PIA guidance from other sources and jurisdictions

- Government of Ontario, ***Freedom of Information and Protection of Privacy Manual***
- Government of Ontario Recordkeeping, Access and Privacy Advisory Services at 416-327-1600 or **access.privacy@ontario.ca**
- United Kingdom Information Commissioner's Office, **Data protection impact assessments** (2023)
- Office of the Australian Information Commissioner, **Guide to Undertaking PIAs** (2021)
- United States Department of Justice, **Impact Assessment Guidance**

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The Information and Privacy Commissioner of Ontario oversees compliance with several laws, which protect the access and privacy rights of Ontarians. These laws include:

- ***Freedom of Information and Protection of Privacy Act*** **(FIPPA)**
- ***Municipal Freedom of Information and Protection of Privacy Act*** **(MFIPPA)**
- ***Personal Health Information Protection Act*** **(PHIPA)**
- **Part X of the *Child, Youth and Family Services Act* (CFYSA)**
- ***Anti-Racism Act***

The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under these acts, the commissioner:

- **resolves access to information appeals**
- **investigates privacy complaints**
- **provides comment on proposed government legislation and programs**
- **reviews organizations' privacy policies and information management practices**
- **conducts research into access and privacy issues**
- **educates the public, media and other interested parties about Ontario's access and privacy laws and current issues affecting access and privacy**

Planning for Success:
Privacy Impact Assessment Guide for Ontario's Public Institutions

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

August 2026

Freedom of Information and Access to Records Policy

1. PURPOSE

The Township of Armour is committed to providing access to municipal information in a manner that promotes openness, transparency, accountability, and public confidence while protecting personal privacy.

The purpose of this Policy is to establish the framework for administering requests for access to records in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), as amended.

This Policy complements the Township's Routine Disclosure and Active Dissemination of Municipal Records Policy (ADM-007), which provides access to records that are routinely available without the need for a formal Freedom of Information request.

2. SCOPE

This Policy applies to all records in the custody or under the control of the Township of Armour that are subject to the access provisions of MFIPPA, regardless of format, location, or storage medium.

Records may include, but are not limited to:

- Paper records;
- Electronic documents;
- Electronic mail (email);
- Audio and video recordings;
- Photographs;
- Databases and information systems;
- Cloud-based records;
- Geographic Information System (GIS) records; and
- Records created, received, stored, processed, or maintained using emerging technologies, including artificial intelligence systems, where such records are under the custody or control of the Municipality.

This Policy applies to all Members of Council, officers, employees, volunteers, contractors, consultants, and any other individual acting on behalf of the Municipality.

3. DEFINITIONS

For the purposes of this Policy, the following definitions apply:

"Act" means the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), as amended from time to time, and any applicable regulations made under the Act.

"Applicant" means a person who makes a formal request for access to records under MFIPPA.

"Custody or Control" means the authority of the Township to manage, retain, use, disclose, or otherwise exercise control over a record, whether the record is physically held by the Township or by another party on behalf of the Township.

"Head" means the individual designated as the head of the institution under MFIPPA or otherwise authorized through a lawful delegation of authority.

"Information and Privacy Commissioner of Ontario (IPC)" means the independent oversight body responsible for reviewing decisions and investigating matters relating to access to information and protection of personal privacy under MFIPPA.

"Municipal Record" means any recorded information, regardless of format or storage medium, that is created, received, maintained, or controlled by the Township in the course of municipal business.

"Personal Information" means recorded information about an identifiable individual as defined under MFIPPA.

"Routine Disclosure" means the regular release of certain municipal records or information without requiring a formal access request under MFIPPA.

"Third Party" means a person, group of persons, or organization other than the applicant or the Township that may have an interest in records responsive to an access request.

4. LEGISLATIVE AUTHORITY

This Policy shall be administered in accordance with:

- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), as amended;
- Applicable regulations;
- Orders, decisions, guidance, and best practices issued by the Information and Privacy Commissioner of Ontario (IPC); and
- Any other applicable legislation.

Where this Policy conflicts with applicable legislation, the legislation shall prevail.

5. RESPONSIBILITIES

Council approves this Policy and any amendments and support the Township's commitment to openness, accountability, transparency, and privacy protection.

Department Heads shall ensure records are created, maintained, and managed in accordance with approved records management practices; ensure records documenting municipal decisions and business activities are complete and accurate; assist in identifying and retrieving responsive records; conduct or co-ordinate reasonable searches for records; preserve records that may be responsive to an access request; protect confidential and personal information; and support compliance with this Policy and applicable legislation.

The Clerk/Privacy Officer shall administer this Policy and perform the duties assigned by the Head under MFIPPA and any applicable delegation of authority. The Clerk is responsible for co-ordinating formal access requests; providing advice and guidance on access to information and privacy matters; assisting applicants and facilitating access in accordance with MFIPPA; consulting with Department Heads, third parties, and other institutions where required; issuing or co-ordinating decisions in accordance with delegated authority; maintaining Freedom of Information request records; monitoring compliance with MFIPPA, this Policy, and related procedures; and promoting continuous improvement of access and privacy practices. Administrative procedures may be established by the Clerk to support the implementation of this Policy.

Employees shall co-operate in responding to access requests; maintain records in accordance with Township policies and procedures; create and maintain complete and accurate records relating to municipal business activities; protect confidential and personal information; preserve records that may be responsive to an access request; and comply with this Policy and applicable legislation.

Records Access and Privacy Designate is a position that may be designated by the Clerk to one or more Township employees to assist with the administrative and operational responsibilities associated with the administration of Freedom of Information requests and the Township's records access and privacy obligations. Assigned duties may include receiving and tracking access requests, coordinating records searches with Department Heads, gathering and organizing responsive records, preparing records for review and disclosure, coordinating applicant correspondence, maintaining request files and documentation, assisting with fee estimates and processing, supporting records management activities, and assisting with other administrative requirements under this Policy. The Records Access and Privacy Designate shall perform assigned duties under the direction and oversight of the Clerk. The designation does not establish a separate statutory office or transfer the statutory responsibilities or decision-making

authority of the Head under MFIPPA. All decisions, approvals, and determinations requiring the authority of the Head or Clerk shall remain with the Clerk unless otherwise authorized by law.

6. POLICY STATEMENT

The Township of Armour shall administer requests for access to records in accordance with MFIPPA and is committed to:

- Providing access to municipal records in a fair, consistent, transparent, and timely manner;
- Promoting access by default through routine disclosure and active dissemination wherever appropriate;
- Protecting the privacy of personal information;
- Supporting transparency and accountability in municipal government;
- Making every reasonable effort to assist applicants and respond openly, accurately, and completely;
- Conducting reasonable searches for responsive records;
- Maintaining accurate, complete, and reliable municipal records;
- Processing timelines and Staged Access Plans calculated using the mandatory business-day standards defined by the latest MFIPPA amendments, establishing a standard baseline response window of 45 business days;
- Applying legislative exemptions only where authorized or required by law; and
- Continuously improving access to information and privacy practices.

7. RECORDS MANAGEMENT

Effective records management is essential to transparency, accountability, and access to information.

All municipal records shall be created, received, classified, maintained, retained, archived, and disposed of in accordance with the Township of Armour's Records Retention By-law, records management policies, and applicable legislation.

The Township shall maintain records in a manner that supports timely retrieval, appropriate access, and protection of information.

8. DUTY TO ASSIST AND ACCESS SUPPORT

The Township shall make every reasonable effort to assist applicants, provide accurate information, clarify requests where appropriate, and facilitate access to records in accordance with MFIPPA.

The Township shall consider whether records can be provided through routine disclosure, active dissemination, partial disclosure, or other appropriate means before requiring a formal access process.

The Clerk may assign the Records Access and Privacy Designate to assist with coordinating applicant communications, clarifying requests, facilitating records searches, and supporting the processing of access requests under the direction of the Clerk.

9. RESEARCH REQUESTS AND REQUIRED DOCUMENTATION

Where an applicant or researcher requests access to personal information for research purposes, the Township shall ensure that the request is reviewed in accordance with MFIPPA and applicable Information and Privacy Commissioner of Ontario (IPC) guidance.

Prior to any disclosure of personal information for research purposes, the following documents are mandatory and must be completed and approved:

- The applicable Information and Privacy Commissioner of Ontario (IPC) research request form;
- A Researcher Agreement approved by the Township; and
- Any other documentation or forms required by the IPC, MFIPPA, applicable regulations, or the Township.

10. FEES

The Township shall charge fees for formal access requests in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and applicable regulations.

A mandatory application fee of $5.00 shall be paid by the applicant when submitting a formal access request.

Additional fees may be charged where permitted by MFIPPA, including:

- Photocopies and computer printouts: $0.25 per side;
- Records provided on USB: $10.00 per USB;
- Manual search time: $7.50 per 15 minutes;
- Preparing records for disclosure, including severing exempt information: $7.50 per 15 minutes;
- Developing a computer program or other method of producing a record from a machine-readable record: $15.00 per 15 minutes; and
- Other allowable costs incurred in locating, retrieving, processing, copying, or shipping records where authorized by MFIPPA and applicable regulations.

Where fees prescribed under MFIPPA or its regulations change, the applicable legislated rates shall apply.

The Township shall explicitly provide a formal fee estimate for any anticipated costs exceeding $25.00, informing the requester of their right to request a fee waiver and pausing the statutory response clock until the fee matter is resolved. Where the estimated fee is $100 or more, the Township may require a deposit in accordance with applicable legislation.

The Township shall not charge search or preparation fees for requests for an individual's own personal information, as restricted by MFIPPA.

Fees shall not be used as a barrier to access. The Township may consider fee waivers where permitted by MFIPPA and where it is fair and equitable to do so.

All fee estimates, payments, waivers, and related decisions shall be documented and retained as part of the access request file.

11. PRIVACY PROTECTION

The Township shall protect personal information in its custody or control by collecting, using, disclosing, retaining, and disposing of personal information in accordance with MFIPPA and other applicable legislation.

The Township shall take reasonable steps to ensure personal information is accurate, complete, appropriately used, and protected throughout its lifecycle.

Reasonable administrative, physical, and technical safeguards shall be maintained to protect personal information from unauthorized access, use, disclosure, alteration, or destruction.

12. REVIEWS AND APPEALS

Individuals have the right to request a review of decisions made under MFIPPA by the Information and Privacy Commissioner of Ontario.

The Township shall co-operate with the Information and Privacy Commissioner throughout any review, mediation, or adjudication process and shall comply with applicable orders issued under the Act.

13. ANNUAL REPORTING

The Clerk shall maintain records and prepare reports as required by MFIPPA and applicable regulations, with administrative and reporting assistance provided by the Records Access and Privacy Designate where assigned. The Clerk may provide periodic reports to Council regarding

access to information activities, privacy compliance, trends, risks, and other matters related to the Township's Privacy Management Program.

14. REVIEW

The Clerk shall review this Policy periodically to ensure continued compliance with legislative requirements, municipal best practices, Information and Privacy Commissioner guidance, and operational needs.

15. EFFECTIVE DATE

This Policy comes into effect on the date approved by Council.

DISTRICT OF PARRY SOUND

OFFICE OF THE MUNICIPAL CLERK

56 ONTARIO STREET
PO BOX 533
BURK'S FALLS, ON
P0A 1C0

(705) 382-3332
(705) 382-2954
Fax: (705) 382-2068
Email: clerk@armourtownship.ca
Website: www.armourtownship.ca

Standard FOI Fee Invoice Template

This ensures the Township fully recovers its administrative costs.

THE MUNICIPAL CORPORATION OF THE TOWNSHIP OF ARMOUR
56 Ontario Street, PO Box 250, Burk's Falls, ON P0A 1C0

INTERIM FEE ESTIMATE / FINAL INVOICE FOR ACCESS TO RECORDS

Date: [Insert Date]
FOI File Reference No: FOI-

Applicant Name: [Insert Name]

Pursuant to Section 45 of the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, the fees associated with processing your request for information have been calculated as follows:

Item Description	Rate Structure	Quantity / Time	Line Total
Statutory Application Fee	Mandatory (Non-refundable)	1	$5.00
Manual Search Time	$7.50 per 15 minutes (30/$hr$)		
Record Preparation & Severing	$7.50 per 15 minutes (30/$hr$)		
Photocopies / Hardcopy Prints	$0.25 per page (single side)	[ ] pages	$[ ]
Secure Digital Media Delivery	$10.00 per USB Drive	[ ] drives	$[ ]
Other Allowable Costs	Direct shipping/courier cost	Actual Cost	$[ ]
TOTAL PROCESSING FEE:			**$[ ]**

Notice Regarding Deposits (If applicable):

- ☐ The total estimated fee for your request is **under $100.00**. Full payment is required upon or before the release of records.
- ☐ The total estimated fee for your request is **$100.00 or more** ($***). In accordance with municipal policy, a 50% deposit ($***) is required before further record search or processing actions can continue. The legislative response clock is paused until this deposit is received.

Privacy Breach Response Policy

1. PURPOSE

The purpose of this Policy is to establish the Township's framework for identifying, containing, investigating, assessing, reporting, and responding to actual or suspected privacy breaches involving personal information. The Township is committed to protecting personal information entrusted to it and ensuring that privacy breaches are managed in a timely, consistent, transparent, and accountable manner.

This Policy is guided by:

- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
- Applicable regulations;
- Guidance and recommendations issued by the Information and Privacy Commissioner of Ontario (IPC); and
- Established privacy and information security best practices.

This Policy establishes procedures to:

- Minimize harm to affected individuals;
- Ensure prompt containment of privacy breaches;
- Assess whether a breach creates a real risk of significant harm;
- Determine notification and reporting obligations;
- Document decisions and response actions; and
- Implement corrective measures to prevent recurrence.

This Policy applies to:

- All Township employees;
- Members of Council;
- Appointed officials;
- Volunteers;
- Contractors, consultants, and service providers;
- All Township departments and operational units;
- All records containing personal information, including paper, electronic, audio, video, and cloud-based records; and
- All information systems, applications, artificial intelligence systems, automated tools, and third-party platforms used to process personal information.

This Policy applies to both suspected and confirmed privacy breaches.

2. DEFINITIONS

"Personal Information" means recorded information about an identifiable individual as defined under MFIPPA.

"Privacy Breach" means an incident involving the unauthorized collection, access, use, disclosure, retention, loss, or destruction of personal information contrary to MFIPPA, applicable law, Township policy, or established procedures.

Examples include:

- Unauthorized access to personal information;
- Unauthorized disclosure by email, mail, verbal communication, or electronic transmission;
- Lost or stolen documents, devices, or storage media;
- Cybersecurity incidents, including phishing, malware, ransomware, or hacking;
- Improper disposal of records;
- Unauthorized access by employees, contractors, or third parties;
- Improper use of personal information; and
- Unauthorized disclosure through artificial intelligence tools or automated systems.

A privacy breach may be accidental or intentional.

"Suspected Privacy Breach" is an event where there is reason to believe that personal information may have been accessed, used, disclosed, lost, or compromised without authorization.

"Real Risk of Significant Harm (RROSH)" means a real risk that a breach could result in significant harm to an affected individual, including bodily harm, humiliation, damage to reputation or relationships, loss of employment or business opportunities, or financial loss.

Potential harms include:

- Identity theft or fraud;
- Financial loss;
- Physical harm or safety risks;
- Emotional distress;
- Reputational harm;
- Discrimination or embarrassment;

- Loss of employment, professional, educational, or personal opportunities;
- Exposure of sensitive personal circumstances; or
- Increased risk to vulnerable individuals.

"Head" means the head of the institution as defined under MFIPPA, or an individual authorized to exercise delegated authority on behalf of the Head.

"Privacy Officer" is the Township official responsible for co-ordinating privacy compliance activities, including privacy breach response, investigations, documentation, and liaison with the IPC. The Privacy Officer acts in an advisory and co-ordinating capacity and does not replace the statutory authority or responsibilities of the Head under MFIPPA.

"Privacy Breach Response Team" is the group of Township personnel responsible for co-ordinating breach response activities. Membership may include:

- Privacy Officer;
- Clerk or designate;
- Information Technology representatives;
- Records management personnel;
- Communications personnel;
- Legal counsel; and
- Other subject matter experts as required.

3. PRIVACY BREACH RESPONSE PRINCIPLES

The Township shall respond to privacy breaches according to the following principles:

- Immediate containment of unauthorized access, use, or disclosure;
- Protection of affected individuals;
- Prompt assessment of risk and potential harm;
- Accountability and transparency;
- Compliance with MFIPPA and IPC guidance;
- Appropriate notification where required;
- Accurate documentation of all decisions and actions; and
- Continuous improvement of privacy safeguards.

4. REPORTING A PRIVACY BREACH

4.1 Duty to Report

All employees, Council members, volunteers, contractors, and service providers must immediately report any suspected or confirmed privacy breach.

Reports shall be made to:

- The employee's supervisor;
- The Privacy Officer; and/or
- Designated Information Technology or records management personnel.

Employees are not expected to determine whether a breach has occurred before reporting.

5. IMMEDIATE CONTAINMENT

5.1 Requirement to Contain

Upon discovery or suspicion of a privacy breach, immediate action shall be taken to contain the breach and prevent further unauthorized access, use, or disclosure. Containment shall begin without waiting for completion of the investigation.

5.2 Containment Measures

Depending on the circumstances, containment measures may include:

- Securing affected records or locations;
- Retrieving improperly disclosed information where possible;
- Requesting deletion or return of information disclosed to unauthorized recipients;
- Isolating affected systems;
- Disabling compromised accounts;
- Revoking access privileges;
- Changing passwords or credentials;
- Preserving evidence;
- Restricting further disclosure; and
- Notifying appropriate technical or administrative personnel.

6. PRIVACY BREACH INVESTIGATION

6.1 Investigation Responsibility

All suspected or confirmed privacy breaches shall be investigated under the direction of the Privacy Officer. The Privacy Officer co-ordinates the investigation and response process. Statutory responsibilities under MFIPPA remain with the Head of Institution.

6.2 Investigation Objectives

The investigation shall determine:

- What occurred and when;
- How the breach occurred;
- The type of personal information involved;
- The sensitivity of the information;
- The individuals affected or potentially affected;
- The extent of unauthorized access, use, disclosure, retention, copying, or distribution;
- Whether the information remains at risk;
- Whether unauthorized recipients have retained or further disclosed information;
- Whether notification obligations exist; and
- Required corrective actions.

6.3 Investigation Activities

The investigation may include:

- Interviews with individuals involved;
- Review of system logs and access records;
- Examination of emails and electronic records;
- Review of physical record handling procedures;
- Consultation with IT security personnel;
- Consultation with vendors or service providers;
- Legal review where appropriate; and
- Assessment of existing privacy and security controls.

6.4 Investigation Documentation

The investigation record shall include:

- Date and time the breach occurred, if known;
- Date discovered;
- Timeline of events;
- Nature and scope of the breach;
- Information involved;
- Individuals affected;
- Evidence reviewed;
- Decisions made;
- Notifications issued; and
- Corrective actions taken.

7. PRIVACY BREACH RISK ASSESSMENT

7.1 Assessment Requirement

Every confirmed privacy breach shall be assessed to determine:

- Whether a real risk of significant harm exists;
- Whether affected individuals should be notified;
- Whether notification to the IPC is required or appropriate; and
- Whether additional mitigation measures are required.

7.2 Assessment Factors

The Township shall consider:

- Sensitivity of the personal information;
- Number of individuals affected;
- Likelihood that the information has been, is being, or will be misused;
- Nature of the unauthorized access, use, or disclosure;
- Whether the information has been recovered or contained;
- Whether the breach resulted from unauthorized internal or external activity;
- Availability of measures individuals can take to reduce harm;
- Whether the breach is systemic or recurring; and
- Applicable MFIPPA requirements and IPC guidance.

7.3 Risk Assessment Record

The Privacy Officer shall maintain documentation of the assessment, including:

- Summary of the incident;
- Risk analysis;
- RROSH determination;
- Notification decision;
- Reasoning supporting the decision; and
- Approval or review by appropriate Township officials.

8. NOTIFICATION REQUIREMENTS

8.1 Notification to the IPC

Where a privacy breach involves a real risk of significant harm (RROSH), the Township shall legally notify the Information and Privacy Commissioner of Ontario (IPC) as soon as practicable.

The Privacy Officer, or designate, shall complete the IPC's *Report a Privacy Breach at Your Organization* form and provide all available information regarding the breach.

The notification shall include available information regarding:

- The nature of the breach;
- Personal information affected;
- Number of individuals affected;
- Circumstances of the breach;
- Containment measures;
- Corrective actions; and
- Contact information for Township representatives.

8.2 Notification to Affected Individuals

Where a privacy breach creates a real risk of significant harm, the Township shall notify affected individuals as soon as reasonably practicable.

Notification shall include:

- A description of the breach;
- Date or timeframe of the breach, where known;
- Type of personal information involved;

- Steps taken to contain and address the breach;
- Recommended actions individuals may take to reduce potential harm;
- Township contact information; and
- Information regarding the right to make a complaint to the IPC.

Notifications shall be written in clear and plain language.

8.3 Method of Notification

The Township shall generally provide direct notification to affected individuals.

Indirect notification may be considered only where direct notification is impractical or inappropriate, including situations involving:

- Large numbers of affected individuals;
- Inability to identify affected individuals;
- Inaccurate or unavailable contact information; or
- Other exceptional circumstances.

The rationale for indirect notification shall be documented.

9. THIRD-PARTY AND VENDOR BREACHES

Where contractual arrangements permit, the Township shall require third-party service providers, contractors, or vendors involved in a privacy breach to:

- Immediate notification to the Township (without undue delay);
- Co-operation with investigation activities;
- Disclosure of the scope and impact of the breach;
- Preservation of evidence;
- Assistance with notification requirements; and
- Implementation of corrective measures.

Contracts should include appropriate privacy, confidentiality, security, and breach notification obligations.

10. CORRECTIVE AND PREVENTATIVE MEASURES

10.1 Remediation

Following investigation, the Township shall implement appropriate corrective actions, which may include:

- System security improvements;
- Access control changes;
- Credential resets;
- Data recovery or secure destruction;
- Policy updates;
- Process improvements; and
- Additional safeguards.

10.2 Prevention of Recurrence

Preventative measures may include:

- Privacy and security training;
- Updated procedures;
- Enhanced monitoring;
- Improved vendor controls;
- Technology upgrades;
- Encryption improvements; and
- Additional audits or reviews.

10.3 Disciplinary Measures

Where a breach results from negligence, misconduct, or failure to follow Township requirements, appropriate disciplinary or contractual action may be taken.

10.4 Post-Incident Review

Significant breaches shall undergo a post-incident review to evaluate:

- Root causes;
- Effectiveness of the response;
- Adequacy of safeguards;
- Employee awareness and training;
- Vendor controls;
- Policy effectiveness; and
- Required improvements.

11. PRIVACY BREACH RECORDS AND ACCOUNTABILITY

The Township shall maintain a confidential Privacy Breach Log. The log shall document:

- Date and nature of the breach;

- Personal information involved;
- Individuals affected;
- Risk assessment;
- Notifications provided;
- Response actions;
- Corrective measures; and
- Final outcome.

Records shall be retained in accordance with Township retention schedules, MFIPPA requirements, and applicable records management practices.

12. POLICY REVIEW

This Policy shall be reviewed periodically to ensure continued alignment with MFIPPA, Information and Privacy Commissioner of Ontario (IPC) guidance and decisions, privacy protection requirements, cybersecurity best practices, emerging technologies, and municipal operational needs. The Township shall update this Policy as required to maintain effective privacy breach management practices.

13. EFFECTIVE DATE

This Policy comes into effect on the date approved by Council.

DISTRICT OF PARRY SOUND

56 ONTARIO STREET
PO BOX 533
BURK'S FALLS, ON
P0A 1C0

(705) 382-3332
(705) 382-2954
Fax: (705) 382-2068
Email: clerk@armourtownship.ca
Website: www.armourtownship.ca

Township of Armour

Privacy Breach Reporting Form

(Confidential – To be completed immediately upon discovery or suspicion of a privacy breach)

SECTION 1 – INCIDENT DETAILS

Date of Report: _____
Time Reported: _____

Date Breach Occurred (if known): _____
Time Breach Occurred (if known): _____

Reported By (Name & Position): _____

Department / Division: _____

Contact Information (phone/email): _____

SECTION 2 – TYPE OF INCIDENT (CHECK ALL THAT APPLY)

☐Unauthorized access to records
☐Unauthorized disclosure of personal information
☐Lost or stolen records (paper or electronic)
☐Cybersecurity incident (phishing, malware, ransomware, hacking)
☐Accidental disclosure (email, mail, verbal, system error)
☐Improper disposal of records
☐Social media disclosure error
☐Vendor/third-party breach
☐Other: _____

SECTION 3 – DESCRIPTION OF BREACH

Provide a clear summary of what occurred:

- What happened?

_____
_____

- How was the breach discovered?

_____
_____

- When did it occur?

_____
_____

- Where did it occur (system, department, location)?

_____

SECTION 4 – INFORMATION INVOLVED

Type of information involved (check all that apply):

☐ Personal information (general)
☐ Sensitive personal information (health, financial, etc.)
☐ Employee information
☐ Council / closed session information
☐ FOI-related records (MFIPPA request materials)
☐ Operational / administrative records
☐ Other: _____

Description of Information Affected:

_____

_____

_____

Approximate Number of Individuals Affected:

☐ 1
☐ 2–10
☐ 11–50
☐ 51–100
☐ 100+
☐ Unknown at this time

SECTION 5 – CONTAINMENT ACTIONS TAKEN

Immediate actions taken to contain the breach:

_____

_____

Has access been restricted or revoked?
☐ Yes
☐ No
☐ In progress

Has IT/security been notified?
☐ Yes
☐ No

Has the breach been stopped or is it ongoing?
☐ Stopped
☐ Ongoing
☐ Unknown

SECTION 6 – RISK ASSESSMENT (INITIAL)

Likelihood of Harm:

☐ Low
☐ Moderate
☐ High
☐ Unknown

Type of Potential Harm (check all that apply):

☐ Identity theft
☐ Financial fraud
☐ Reputational harm
☐ Emotional or personal distress
☐ Loss of confidentiality
☐ Operational disruption
☐ Other: _____

SECTION 7 – NOTIFICATION REQUIREMENTS

Internal Notification Completed:

☐ Clerk (Privacy Officer)
☐ Department Head
☐ IT Services
☐ Legal Counsel (if applicable)

Date/Time Notifications Made: _____

External Notification Required? (Initial Assessment)

☐ Yes
☐ No
☐ Under Review

If Yes (check all that apply):

☐ Affected individuals
☐ Information and Privacy Commissioner of Ontario (IPC)
☐ Law enforcement
☐ External regulator
☐ Vendor/third party

SECTION 8 – ROOT CAUSE (IF KNOWN)

☐ Human error
☐ System failure
☐ Policy/process gap
☐ Malicious activity
☐ Third-party/vendor error
☐ Unknown at this time

Details:

SECTION 9 – CORRECTIVE ACTIONS (IMMEDIATE & PLANNED)

Immediate corrective actions taken:

Planned corrective actions:

SECTION 10 – DOCUMENTATION & EVIDENCE

List any supporting materials collected:

☐ Emails
☐ Screenshots
☐ System logs
☐ Physical documents
☐ Vendor reports
☐ Other: _____

Location of stored evidence:

SECTION 11 – VENDOR INVOLVEMENT (IF APPLICABLE)

Is a third-party/vendor involved?

☐ Yes
☐ No

Vendor Name:

Has vendor been notified?
☐ Yes
☐ No

Vendor response summary:

SECTION 12 – CLERK / PRIVACY OFFICER REVIEW

Risk classification confirmed:
☐ Low
☐ Moderate
☐ High

Final determination:
☐ No breach
☐ Confirmed breach – no notification required
☐ Confirmed breach – notification required

Notification actions authorized:

Date Reviewed: _____
Reviewed By: _____

SECTION 13 – POST-INCIDENT ACTIONS (TO BE COMPLETED LATER)

☐ Policy update required
☐ Staff training required
☐ System/security improvements required
☐ Vendor contract review required
☐ Process redesign required

SECTION 14 – SIGN-OFF

Report Completed By:

Signature: _____ Date: _____

Clerk / Privacy Officer Approval:

Signature: _____ Date: _____

CONFIDENTIALITY NOTICE

This form contains sensitive information and must be handled in accordance with the Township of Armour Privacy Management Program and MFIPPA requirements. Unauthorized disclosure is prohibited.

Township of Armour

Privacy Breach Response Policy – Appendix A

Privacy Breach Notification Decision Tree

Step 1 – Is this a confirmed or suspected privacy breach?

A breach includes any:

- Unauthorized access to personal information
- Unauthorized disclosure (intentional or accidental)
- Loss or theft of records containing personal information
- Cybersecurity incident affecting municipal data
- Vendor or third-party exposure of Township data

Decision:

- ☐ No → No breach process required
- ☐ Yes → Proceed to Step 2

Step 2 – What type of information is involved?

Check all that apply:

- ☐ Basic contact information only (name, address, phone)
- ☐ Employee or HR information
- ☐ Financial information
- ☐ Health or medical information
- ☐ Social services / sensitive personal information
- ☐ Council closed session / confidential municipal information
- ☐ Multiple categories or unknown

IPC Risk Indicator:

- Basic contact info only → Lower risk
- Sensitive personal information → Higher risk

Step 3 – How many individuals are affected?

- ☐ 1 individual
- ☐ 2–10 individuals
- ☐ 11–100 individuals
- ☐ 100+ individuals
- ☐ Unknown / potential systemic exposure

IPC Risk Indicator:

- Small scale → lower risk
- Large scale or unknown → higher risk

Step 4 – Is there a reasonable risk of harm? (KEY IPC TEST)

Consider:

- Could the information be used for identity theft or fraud?
- Could it cause financial loss?
- Could it cause reputational or emotional harm?
- Is the information now accessible outside Township control?
- Is the data unencrypted or easily usable?

Decision:

- ☐ No reasonable risk of harm → LOW RISK
- ☐ Possible harm but limited → MODERATE RISK
- ☐ Likely or significant harm → HIGH RISK

Step 5 – Is the breach contained?

- ☐ Yes – fully contained (access removed, email recalled, system secured)
- ☐ Partially contained
- ☐ Not contained / ongoing incident

Step 6 – IPC Reporting Requirement Decision

LOW RISK BREACH

Characteristics:

- Non-sensitive information
- Limited individuals affected
- No reasonable risk of harm
- Fully contained

Action:

- No IPC notification required
- Document internally
- Notify individuals if appropriate

MODERATE RISK BREACH

Characteristics:

- Some sensitive information OR
- Limited risk of harm OR
- Small to moderate number of individuals

Action:

- Notify Clerk/Privacy Officer immediately
- Notify affected individuals (case-by-case assessment)
- Consider IPC notification if escalation risk exists
- Document full incident

HIGH RISK BREACH (IPC REPORTING TRIGGER)

Characteristics include ANY of the following:

- Sensitive personal information involved
- Likely risk of identity theft, fraud, or harm
- Large number of individuals affected
- Cybersecurity incident (hacking, ransomware, unauthorized system access)
- Vendor or cloud service breach
- Systemic or repeated failure
- Information exposed beyond Township control

Action:

- 🚨 **Immediate notification to Clerk / Privacy Officer**
- 🚨 **Notify Information and Privacy Commissioner of Ontario (IPC) without delay**
- 🚨 Notify affected individuals
- 🚨 Initiate full breach investigation and containment plan

Step 7 – Mandatory Internal Escalation (All Levels)

Regardless of risk level:

- Clerk / Privacy Officer must be notified immediately
- IT Services must be engaged where systems are involved
- Legal counsel may be engaged for high-risk or complex breaches
- Vendor notification required if third party is involved

Step 8 – Final Determination Authority

Final classification (Low / Moderate / High risk and IPC notification decision) rests with:

The Clerk, as Privacy Officer under MFIPPA

All decisions must be:

- Documented
- Justified based on risk factors
- Retained as part of breach file (linked to FOI Code A11 if applicable)

Quick Reference Summary

Risk Level	IPC Notification	Internal Action
Low	Not required	Document only
Moderate	Case-by-case	Notify individuals + monitor
High	REQUIRED	IPC + individuals + full response

Key IPC Principle Embedded in This Tool

A privacy breach must be reported externally when there is a **real risk of significant harm**, not merely when a breach occurs.

DISTRICT OF PARRY SOUND

OFFICE OF THE MUNICIPAL CLERK

56 ONTARIO STREET
PO BOX 533
BURK'S FALLS, ON
P0A 1C0

(705) 382-3332
(705) 382-2954
Fax: (705) 382-2068
Email: clerk@armourtownship.ca
Website: www.armourtownship.ca

Confidential Municipal Privacy Breach Log

The Municipal Corporation of the Township of Armour
Restricted Access: Clerk / Privacy Officer & CAO Only

Executive Summary Tracker

- **Total Confirmed Breaches (YTD):** [0]
- **Total Suspected Breaches (Cleared):** [0]
- **Open Investigations:** [0]
- **Incidents Reported to IPC:** [0]

Active Breach Registry

Incident Reference: PB-2026-001 *(Example Entry)*

	Registry Details
Status	□ Closed / □ Under Investigation / □ Escalated to IPC
Date & Time Occurred	YYYY-MM-DD at 00:00 AM/PM *(or "Unknown - Historical")*
Date & Time Discovered	YYYY-MM-DD at 00:00 AM/PM
Reported By	[Name and Position of staff member / vendor who flagged it]
Responsible Department	[e.g., Treasury, Public Works, Fire Services, Building]

1. Incident Description

What Happened: [Provide a concise, factual summary of the event. Avoid emotional language. e.g., "An employee accidentally emailed an unredacted property tax account ledger containing financial details to an incorrect resident due to an autocomplete error in Outlook."]

Format of Data: ☐ Physical Paper | ☐ Digital/Email | ☐ Cloud System | ☐ AI/Emerging Tech

TOWNSHIP OF ARMOUR
OFFICE OF THE MUNICIPAL CLERK

DISTRICT OF PARRY SOUND

56 ONTARIO STREET
PO BOX 533
BURK'S FALLS, ON
P0A 1C0

(705) 382-3332
(705) 382-2954
Fax: (705) 382-2068
Email: clerk@armourtownship.ca
Website: www.armourtownship.ca

2. Scope & Sensitivity of Personal Information

Types of Data Exposed: ☐ Names |☐ Addresses |☐ Financial/Banking | ☐ Health/Medical | ☐ Employee Records | ☐ Other: `[List here]`

Volume: Total number of individuals affected: `[e.g., 1 individual / 45 residents]`

Vulnerable Populations: Does this involve children, elderly residents, or vulnerable persons registries? ☐ Yes | ☐ No

3. 4-Step Response Execution Timeline

Step 1: Containment (Within 24 Hours)
Action Taken: [e.g., "Contacted the unintended recipient via phone and email within 4 hours. Recipient confirmed in writing that the email was deleted from their inbox and trash folder without being copied or distributed."]
Date Completed: YYYY-MM-DD

Step 2: Investigation & Risk Assessment
Real Risk of Significant Harm (RROSH) Determination: ☐ Low Risk / ☐ Moderate Risk / ☐ High Risk
Rationale: [e.g., "Low Risk. Data was contained quickly with a verified recipient who complied with deletion instructions. Harm or identity theft is highly unlikely."]

Step 3: Notification Metrics
Affected Individuals Notified? ☐ Yes (Sent via: Direct Mail) | ☐ No (Provide rationale)
IPC Notified? ☐ Yes (IPC Ref #: _____) | ☐ No (Did not meet RROSH threshold)

Step 4: Remediation & Prevention (Post-Incident)
System/Process Adjustments: [e.g., "Disabled Outlook external email autocomplete for the treasury system workstation. Conducted a 5-minute refresher training on verifying email attachments with the affected employee."]

Date Signed Off by CAO: YYYY-MM-DD

Artificial Intelligence and Emerging Technology Policy

1. PURPOSE

The purpose of this Policy is to establish a responsible, ethical, transparent, and accountable framework for the use of Artificial Intelligence (AI) and emerging technologies by the Township of Armour ("the Township").

The Township recognizes that AI and emerging technologies may provide opportunities to improve municipal operations, enhance service delivery, increase administrative efficiency, and support cybersecurity initiatives. The Township also recognizes that these technologies may introduce privacy, security, legal, ethical, and operational risks.

This Policy establishes governance requirements to ensure that AI systems are implemented and used responsibly, with appropriate approval, human oversight, protection of municipal information, and consideration of public trust.

This Policy is guided by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), applicable Ontario legislation, guidance issued by the Information and Privacy Commissioner of Ontario (IPC), Ontario government guidance regarding responsible AI use, applicable federal guidance, cybersecurity best practices, and principles of fairness, transparency, accountability, and human oversight.

2. SCOPE

This Policy applies to all Township departments, employees, members of Council, volunteers, contractors, consultants, and third-party service providers.

This Policy applies to all Artificial Intelligence (AI) systems and emerging technologies used, purchased, developed, or accessed for Township purposes, including generative AI, predictive AI, machine learning, automated decision-support systems, chatbots, cybersecurity applications, analytics tools, biometric technologies, and AI-enabled services provided through external vendors.

This Policy applies to AI systems used in municipal operations, service delivery, administrative processes, communications, decision-support activities, and any process involving Township information, municipal records, confidential information, or personal information.

No AI system or emerging technology may be implemented or used for Township purposes without prior approval from the Chief Administrative Officer (CAO).

3. DEFINITIONS

"Artificial Intelligence (AI)" means a machine-based system that uses data and computational methods to infer how to generate predictions, content, recommendations, decisions, or other outputs that can influence physical or digital environments. AI systems may operate with varying degrees of autonomy and may adapt after deployment. For the purposes of this Privacy Management Program, AI includes systems used to collect, analyze, infer, generate, or otherwise process personal information, including machine learning, generative AI, and AI-supported automated decision-making tools.

"Automated Decision-Making" means the use of technology to make, recommend, prioritize, rank, assess, or materially influence decisions affecting individuals or municipal services.

"Emerging Technology" means technology that may introduce new operational, privacy, security, or governance risks, including AI systems, automation tools, biometric technologies, and similar digital solutions.

"Generative AI" means AI systems capable of creating content, including text, images, audio, code, summaries, or analytical outputs based on prompts or input data.

"High-Risk AI Use" means AI applications that may significantly affect individuals, including automated decision-making, biometric applications, or systems involving sensitive personal information.

"Low-Risk AI Use" means AI applications used for administrative assistance, productivity, drafting, summarization, or other functions that do not directly affect individual rights, eligibility, safety, or access to municipal services.

"Personal Information" means recorded information about an identifiable individual as defined under MFIPPA.

"Predictive AI" means AI systems that analyze information and patterns to support forecasting, predictions, or data-informed decision-making.

"Privacy Impact Assessment (PIA)" means an assessment used to identify and address privacy risks associated with the collection, use, disclosure, or processing of personal information.

"Real Risk of Significant Harm (RROSH)" means the threshold used to assess privacy breaches, defined as a real risk of significant harm—such as identity theft, physical harm,

humiliation, damage to reputation or relationships, or financial loss—arising from the unauthorized access, use, or disclosure of personal information.

4. GOVERNANCE AND ACCOUNTABILITY

The Township shall maintain centralized oversight of AI and emerging technologies through the Chief Administrative Officer (CAO), supported by the Clerk (Privacy Officer) or designate.

The CAO is responsible for approving all AI systems and emerging technologies used by the Township, including internally developed tools, purchased software, vendor-provided services, and AI capabilities incorporated into existing technology platforms.

Before approving an AI system, the CAO shall ensure that the proposed technology has a clearly identified municipal purpose, appropriate operational justification, and has undergone suitable privacy, security, legal, and risk reviews. The review process shall consider the type of information involved, potential impacts on individuals, safeguards required, staff training needs, and ongoing monitoring requirements.

No department, employee, contractor, consultant, or service provider shall implement or use an AI system for Township purposes unless approval has been granted by the CAO.

The Clerk (Privacy Officer) or designate shall provide privacy oversight and advice regarding AI systems. This includes reviewing proposed uses for compliance with MFIPPA, advising whether a Privacy Impact Assessment is required, identifying privacy risks, recommending mitigation measures, and maintaining appropriate privacy documentation. The Privacy Officer's role is advisory and does not replace the statutory responsibilities of the Head under MFIPPA.

The Township shall maintain an inventory of approved AI systems, including the system purpose, responsible department, vendor information where applicable, information processed, risk classification, approval status, privacy review status, and applicable monitoring requirements.

5. RESPONSIBLE USE PRINCIPLES

5.1 Transparency

The Township shall use AI systems in a transparent manner. Where AI is used in a meaningful way to support service delivery, communications, or decision-making, appropriate notice may be provided to affected individuals.

Where AI-assisted content is used externally, the Township may include an appropriate disclaimer indicating that AI assistance was used and that human review has occurred.

5.2 Accountability and Human Oversight

AI systems shall support, but not replace, human judgment and municipal authority.

Employees remain responsible for reviewing AI-generated information, ensuring accuracy, and complying with applicable legislation, Township policies, and professional obligations.

Departments remain accountable for decisions and outcomes resulting from the use of AI systems.

5.3 Fairness and Bias Mitigation

The Township shall consider potential bias, discrimination, and unintended impacts when implementing AI systems.

Higher-risk AI systems may require additional review to assess fairness, reliability, accuracy, and potential impacts on individuals or groups.

5.4 Privacy and Data Protection

AI systems shall comply with MFIPPA and applicable privacy requirements.

Personal information belonging to staff, Council members, residents, or other individuals shall not be entered into publicly available AI tools unless the system has been approved by the Township and appropriate privacy, security, and contractual protections are in place.

AI systems shall only collect, use, disclose, or process personal information for authorized municipal purposes.

5.5 Security and Risk Management

AI systems shall be reviewed for cybersecurity risks before implementation.

The Township shall consider risks relating to unauthorized access, disclosure, misuse, vulnerabilities, third-party data handling, and system reliability.

Approved AI tools may be used to support cybersecurity initiatives, including threat detection, phishing prevention, and information security improvements.

5.6 Environmental Awareness

Users should be aware that AI services rely on computing infrastructure, including third-party data centres, which may require significant energy and resource consumption and may have indirect environmental impacts.

6. GENERATIVE AI SYSTEMS

6.1 Permitted Uses

Approved generative AI tools may be used to support administrative tasks, drafting, editing, summarizing non-confidential information, preparing preliminary materials, improving workflow efficiency, and assisting with research and analysis.

Generative AI may also be used for other approved municipal purposes where appropriate safeguards and human oversight are maintained.

All AI-generated content must be reviewed by appropriate Township staff before being relied upon, distributed, or incorporated into official Township materials.

6.2 Restrictions

Generative AI shall not be used to make final municipal decisions, provide unauthorized legal interpretations, replace professional judgment, or create content that has not been appropriately reviewed.

AI-generated information shall not be considered authoritative without human verification.

6.3 Input Restrictions

Employees shall not enter personal information, confidential information, closed-session information, municipal election information, protected records, or sensitive Township information into public or unapproved AI systems.

6.4 Accuracy of AI Outputs

AI-generated information may contain inaccuracies, omissions, outdated information, or fabricated content. Employees shall independently verify factual information, legal

references, financial information, technical advice, and other material before relying upon or distributing AI-generated outputs.

7. APPROVED USES OF ARTIFICIAL INTELLIGENCE

Approved AI systems may be used to support Township operations where there is a demonstrated municipal purpose and approval has been obtained from the CAO.

Approved uses may include administrative support, drafting and editing documents, summarizing non-confidential information, assisting with research and analysis, improving workflow efficiency, supporting accessibility initiatives, enhancing cybersecurity measures, and assisting staff with routine operational tasks.

AI systems may also be used to support public communications, service delivery, and internal business processes where appropriate privacy, security, and operational safeguards are in place.

AI-generated content, recommendations, analysis, or other outputs shall be reviewed by appropriate Township staff before being relied upon for municipal purposes.

AI systems shall not replace the authority, judgment, or accountability of Township employees, Council, or decision-makers.

8. CHATBOTS AND VIRTUAL ASSISTANTS

The Township may use approved AI-enabled chatbots and virtual assistants to improve access to municipal information and services.

All chatbot and virtual assistant systems require prior approval from the CAO and shall undergo appropriate privacy, security, and operational review before implementation.

Chatbots may be used to provide general information, assist individuals in locating Township services, answer routine inquiries, and direct users to appropriate resources.

Chatbots shall not provide binding legal, administrative, or statutory decisions and shall not replace staff involvement in complex, sensitive, or individualized matters.

Where a chatbot collects information from individuals, the Township shall ensure that only information necessary for the approved purpose is collected and that the collection, use, disclosure, and protection of personal information complies with MFIPPA and applicable privacy requirements.

9. AUTOMATED DECISION-MAKING SYSTEMS

Automated decision-making refers to the use of AI or automated systems to make, recommend, prioritize, rank, assess, or materially influence decisions affecting individuals, municipal services, programs, or operations.

Due to the potential impact of automated decision-making systems, all such systems require prior approval from the CAO and enhanced review before implementation.

Before approving an automated decision-making system, the Township shall assess the purpose of the system, the information used, potential impacts on individuals, accuracy and reliability, privacy considerations, cybersecurity risks, potential bias, and available safeguards.

Where automated decision-making systems are used, the Township shall ensure meaningful human oversight is maintained. Staff shall retain the ability to review, question, and override automated outputs where appropriate.

The Township remains responsible for decisions and outcomes resulting from the use of automated systems.

Where appropriate, individuals affected by automated processes may be provided with information regarding the use of the system and available options for review or reconsideration.

10. BIOMETRICS AND IDENTIFICATION TECHNOLOGIES

Biometric technologies are systems that identify or verify individuals using physical or behavioural characteristics, including facial recognition, fingerprint scanning, voice recognition, and similar identification technologies.

Because biometric technologies may present elevated privacy, security, and ethical risks, their use requires prior approval from the CAO and completion of appropriate risk assessments before implementation.

Before approving biometric technologies, the Township shall consider whether the proposed use is necessary, proportionate, supported by a legitimate municipal purpose, and whether less intrusive alternatives are available.

Approved biometric systems shall include appropriate safeguards, including access controls, security protections, audit logging, defined retention and destruction requirements, and restrictions on secondary use.

The Township shall provide appropriate notice where biometric technologies are used in public-facing contexts.

11. RISK ASSESSMENT AND CLASSIFICATION

11.1 Risk Assessment Requirements

All AI systems shall undergo an appropriate risk assessment before implementation to determine the level of review, oversight, and safeguards required.

Risk assessments shall consider factors including the type of information processed, whether personal information is involved, the purpose of the system, potential impacts on individuals, cybersecurity considerations, vendor risks, human oversight requirements, accuracy, reliability, and the potential for bias or unintended consequences.

The level of assessment required shall be proportionate to the risk associated with the AI system.

11.2 Low-Risk AI Systems

Low-risk AI systems are generally those used for administrative assistance, productivity, drafting, summarization, or similar activities that do not directly affect individual rights, eligibility, safety, or access to municipal services.

Low-risk systems still require CAO approval before use and must comply with applicable Township privacy, security, and acceptable-use requirements.

11.3 Moderate-Risk AI Systems

Moderate-risk AI systems include public-facing informational tools, chatbots, operational assistance tools, and systems that process limited information while maintaining appropriate safeguards.

Moderate-risk systems require additional review to confirm privacy, security, accessibility, and operational considerations have been addressed.

11.4 High-Risk AI Systems

High-risk AI systems include systems involving personal information, predictive analytics, automated decision-support, significant service impacts, or processes that may materially affect individuals.

High-risk systems require enhanced privacy and security review, appropriate documentation, ongoing monitoring, and CAO approval before implementation.

11.5 Very High-Risk AI Systems

Very high-risk AI systems include automated decision-making systems affecting individuals, biometric technologies, or other systems presenting significant privacy, legal, ethical, or public trust concerns.

Very high-risk systems require enhanced review, documented justification, appropriate safeguards, and CAO approval before implementation.

12. PROCUREMENT AND THIRD-PARTY AI SYSTEMS

All AI systems obtained through procurement, contracts, subscriptions, or third-party service providers require prior CAO approval before implementation.

The Township shall ensure that agreements involving AI systems address privacy, confidentiality, cybersecurity, data ownership, permitted uses of Township information, breach notification obligations, vendor responsibilities, and secure return or destruction of information where appropriate.

Third-party AI and SaaS vendors shall explicitly adhere to the Township's mandatory privacy breach reporting requirements, providing notification without undue delay (no later than within 24 hours) of any security incident or actual/suspected privacy breach involving Township information, alongside comprehensive impact and data volume metrics necessary for the Township to conduct its Real Risk of Significant Harm (RROSH) assessment and satisfy statutory reporting obligations to the Information and Privacy Commissioner of Ontario (IPC).

Vendor agreements shall address whether Township information may be used for AI model training, analytics, or other secondary purposes. Township information shall not be used for these purposes unless expressly authorized by the Township and supported by appropriate contractual protections.

Third-party AI providers shall be expected to comply with applicable Township privacy and security requirements.

13. RESPONSIBILITIES

13.1 Employees

Employees authorized to use AI systems shall comply with this Policy and use approved AI tools responsibly, ethically, and transparently.

Employees shall protect personal, confidential, and sensitive information, review AI-generated content for accuracy and appropriateness, and report suspected misuse, security concerns, privacy breaches, or violations of this Policy.

Employees shall not use Township-provided AI resources for unauthorized personal purposes.

13.2 Members of Council

Members of Council shall use AI systems responsibly and in accordance with this Policy, confidentiality obligations, and applicable legislation.

Council members shall not enter personal information, confidential information, closed-session information, municipal election information, or protected information into unapproved AI systems.

Township-provided AI resources shall not be used for campaigning, election-related activities, or other unauthorized purposes.

13.3 Department Heads and Supervisors

Department heads and supervisors shall ensure that AI use within their areas of responsibility complies with this Policy.

They shall assess operational risks, ensure approved systems are used appropriately, support responsible AI practices, and report concerns regarding inappropriate use.

13.4 Chief Administrative Officer

The CAO is responsible for approval of all AI systems used by the Township and ensuring appropriate governance, oversight, and accountability.

13.5 Clerk (Privacy Officer)

The Clerk (Privacy Officer) shall monitor legislative and regulatory developments relating to AI and privacy, provide privacy guidance, review privacy implications of AI systems, and recommend updates to this Policy as required.

13.6 Information Technology Support

The Township's information technology function shall support the review of AI systems, assess cybersecurity considerations, assist with technical safeguards, and support appropriate implementation of approved technologies.

14. RECORDS MANAGEMENT

AI-generated content, prompts, outputs, and related documentation shall be managed in accordance with applicable Township records management practices where they are required for legal, accountability, operational, or historical purposes.

Not all AI-generated content, prompts, or outputs will constitute official Township records. Employees shall use appropriate judgment when determining whether AI-generated materials should be retained as part of Township records.

15. TRAINING AND AWARENESS

Employees and members of Council authorized to use AI systems shall be provided with appropriate information and guidance regarding the responsible use of approved AI tools.

Guidance may include information regarding approved AI systems, privacy obligations, confidentiality requirements, cybersecurity considerations, limitations of AI-generated information, human review requirements, and procedures for reporting concerns or incidents.

The Township may provide additional education or awareness opportunities as appropriate to support responsible and effective use of AI technologies.

16. MONITORING, REVIEW, AND COMPLAINTS

The Township shall monitor approved AI systems to ensure continued alignment with operational needs, privacy requirements, cybersecurity expectations, and responsible AI practices.

AI systems may be reviewed periodically to assess performance, accuracy, fairness, security, privacy impacts, and continued suitability.

Where concerns are identified regarding the use of an AI system, including inaccurate, unfair, inappropriate, or unintended outcomes, the Township shall review the matter and take appropriate corrective action where required.

Individuals affected by AI-assisted processes may seek human review or clarification through applicable Township processes.

This Policy shall be reviewed periodically and updated as required to reflect changes in legislation, regulatory guidance, technology, cybersecurity practices, and municipal operational requirements.

17. LEGISLATIVE AND REGULATORY ALIGNMENT

The Township's use of AI and emerging technologies shall be conducted in accordance with applicable legislation, regulations, and guidance, including but not limited to:

- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
- Applicable Ontario legislation and regulations relating to privacy, cybersecurity, and municipal operations;
- Guidance and recommendations issued by the Information and Privacy Commissioner of Ontario (IPC);
- Ontario government guidance regarding responsible use of Artificial Intelligence;
- Applicable federal guidance regarding responsible use of Artificial Intelligence; and
- Other legislation or regulatory requirements applicable to Township operations.

The Township shall monitor legislative and regulatory developments relating to AI and update this Policy as required.

18. COMMUNICATION

This Policy shall be made available to Township employees, members of Council, and applicable contractors and service providers to support awareness and compliance.

Where AI-assisted content is used for external communications or official Township materials, the Township may provide appropriate disclosure indicating that AI tools were used and that the final content was reviewed by authorized Township personnel.

Examples of appropriate AI disclosure statements may include:

- "AI assistance was used in preparing this document. The content has been reviewed by qualified municipal staff."
- "This material was developed with the assistance of AI tools. Human review was completed to ensure accuracy and alignment with municipal requirements."
- "AI tools were used to support drafting and formatting. Final review and approval remain the responsibility of Township staff."

19. EFFECTIVE DATE

This Policy comes into effect on the date approved by Council.

Vendor Privacy and Security Standard Policy

1. PURPOSE

The purpose of this Policy is to establish a comprehensive, risk-based framework governing all vendors, contractors, consultants, service providers, and technology partners (collectively "Vendors") who collect, access, store, process, transmit, or dispose of personal information or municipal records on behalf of the Township of Armour ("the Township").

2. SCOPE

This Policy applies to:

- Cloud service providers and SaaS platforms
- IT service providers and managed service contractors
- Professional consultants and operational contractors
- Communications, marketing, and social media service providers
- Any third-party handling records in the custody or control of the Township

This Policy is designed to ensure compliance with:

- The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Applicable IPC guidance on third-party service providers
- Municipal procurement and accountability standards
- Privacy-by-design and security-by-default principles

3. DEFINITIONS

For the purposes of this Policy:

"Artificial Intelligence (AI)" means a machine-based system that uses data and computational methods to infer how to generate predictions, content, recommendations, decisions, or other outputs that can influence physical or digital environments. AI systems may operate with varying degrees of autonomy and may adapt after deployment. For the purposes of this Privacy Management Program, AI includes systems used to collect, analyze, infer, generate, or otherwise process personal information, including machine learning, generative AI, and AI-supported automated decision-making tools.

"Machine Learning" means technology that enables computer systems to identify patterns in data, learn from experience, and improve performance or make predictions without being explicitly programmed for each specific task. Examples include systems that automatically classify documents, identify trends in data, detect unusual activity, provide recommendations, or assist with tasks such as speech recognition and image analysis.

"Personal Information" means recorded information about an identifiable individual as defined by applicable privacy legislation.

"Records" means recorded information in any format, including paper and electronic records, created, received, or maintained by or on behalf of the Township.

"Real Risk of Significant Harm (RROSH)" means the threshold used to assess privacy breaches, defined as a real risk of significant harm—such as identity theft, physical harm, humiliation, damage to reputation or relationships, or financial loss—arising from the unauthorized access, use, or disclosure of personal information.

"Security Incident" means any event that compromises or may compromise the confidentiality, integrity, or availability of Township information or systems.

"Township Information" means all records and information created, collected, received, accessed, used, stored, processed, transmitted, retained, or disposed of by or on behalf of the Township.

"Vendor" means any contractor, consultant, service provider, supplier, technology provider, or subcontractor that provides services to the Township and has access to Township information or systems.

"Privacy Breach" means the unauthorized access, collection, use, disclosure, loss, alteration, retention, or destruction of personal information.

4. LEGISLATIVE AUTHORITY

This Policy is established pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and shall be administered in accordance with applicable legislation, regulations, municipal policies, records retention requirements, and guidance issued by the Information and Privacy Commissioner of Ontario.

Where legislation imposes more stringent privacy requirements, those requirements shall prevail.

5. RESPONSIBILITIES

Council approves this Policy.

Department Managers are responsible for identifying vendor engagements involving Township information and ensuring compliance with this Policy.

The Clerk/Privacy Officer provides privacy guidance, supports privacy risk assessments, and advises on compliance with MFIPPA.

Procurement ensures appropriate privacy and security requirements are incorporated into procurement documents and agreements.

Information Technology provides technical guidance on information security and technology risks, where applicable.

Vendors are responsible for complying with this Policy and all applicable contractual privacy, security, and confidentiality obligations.

6. VENDOR PRIVACY AND SECURITY PRINCIPLES

All Vendors shall conduct their activities in accordance with the following principles.

6.1 Accountability

Vendors are accountable for protecting all Township information entrusted to them and shall maintain appropriate administrative, technical, and physical safeguards throughout the duration of the contractual relationship.

Compliance with this Standard does not relieve a Vendor of any contractual, statutory, or professional obligations.

6.2 Authorized Collection, Use and Disclosure

Township information shall be collected, accessed, used, disclosed, processed, retained, and disposed of solely for the purposes authorized by the Township and only to the extent necessary to fulfill the applicable contractual obligations.

Information shall not be used for secondary purposes without the Township's prior written authorization.

6.3 Data Minimization

Vendors shall limit the collection, access, use, retention, and disclosure of personal information to the minimum amount reasonably necessary to perform the contracted services.

Where practical, Vendors shall employ privacy-enhancing techniques including anonymization, de-identification, or masking to reduce privacy risks.

6.4 Need-to-Know Access

Access to Township information shall be restricted to personnel whose duties require such access. Vendors shall implement role-based access controls, least-privilege principles, and appropriate authentication mechanisms to prevent unauthorized access.

Access permissions shall be reviewed regularly and promptly revoked when no longer required.

6.5 Security Safeguards

Vendors shall implement safeguards appropriate to the sensitivity, volume, and risk associated with Township information.

Safeguards shall include administrative, technical, and physical measures designed to protect information against unauthorized access, collection, use, disclosure, alteration, destruction, loss, theft, or unavailability.

6.6 Transparency

Vendors shall maintain documented privacy, information security, records management, and incident response practices and shall provide relevant documentation to the Township upon reasonable request.

Vendors shall promptly notify the Township of any material changes to practices that could affect the privacy or security of Township information.

6.7 Privacy by Design and Security by Default

Where technologies or services are developed, implemented, configured, or maintained on behalf of the Township, Vendors shall incorporate privacy and security considerations throughout the system lifecycle.

Default configurations shall protect personal information to the greatest extent reasonably practicable without requiring unnecessary user intervention.

6.8 Risk-Based Information Management

Privacy and security safeguards shall be proportionate to the sensitivity of the information, the likelihood and severity of potential harm, operational requirements, and recognized industry practices.

Higher-risk information shall receive enhanced protection commensurate with the level of risk.

6.9 Continuous Improvement

Vendors shall periodically review and improve their privacy and information security practices to address evolving threats, technological developments, operational changes, and emerging risks.

Where deficiencies are identified, Vendors shall implement corrective measures within reasonable timeframes agreed upon with the Township.

7. VENDOR PRIVACY AND SECURITY REQUIREMENTS

7.1 Contractual Requirements

Vendor agreements involving Township information shall include appropriate privacy, security, confidentiality, and records management requirements based on the nature of the services provided and the sensitivity of the information involved.

7.2 Data Ownership and Control

All Township information remains under the custody and control of the Township. Vendors acquire no ownership rights or independent authority over Township information and shall retain such information only as necessary to provide contracted services or as otherwise required by law.

7.3 Security Safeguards

Vendors shall implement reasonable administrative, technical, and physical safeguards appropriate to the sensitivity and risk of Township information.

Safeguards shall include, where applicable:

- access controls based on least privilege;
- appropriate authentication measures, including multi-factor authentication where required;
- encryption of information in transit and at rest;
- security monitoring and audit logging;
- vulnerability management and security updates; and
- protection against unauthorized access, disclosure, alteration, loss, or destruction.

7.4 Vendor Personnel Requirements

Vendors shall ensure personnel with access to Township information:

- are authorized and require access to perform assigned duties;
- are subject to confidentiality obligations;
- receive appropriate privacy and security training; and
- have access removed promptly when no longer required.

7.5 Privacy Breaches and Security Incidents

Vendors shall notify the Township without undue delay, and no later than within 24 hours, upon becoming aware of any actual or suspected privacy breach or security incident involving Township information.

Vendors shall:

- provide comprehensive impact details, data volume metrics, and sufficient information necessary for the Township to conduct its Real Risk of Significant Harm (RROSH) assessment and satisfy mandatory reporting obligations to the Information and Privacy Commissioner of Ontario (IPC); co-operate with investigation, containment, and remediation activities;
- preserve relevant records, logs, and evidence; and
- provide documentation of actions taken.

7.6 Subcontractors

Vendors shall obtain approval before granting subcontractors access to Township information where required by contract.

Subcontractors shall be subject to privacy, security, confidentiality, and records management obligations equivalent to those imposed on the primary Vendor.

Vendors remain responsible for the actions and compliance of all approved subcontractors.

8. VENDOR RISK MANAGEMENT AND OVERSIGHT

8.1 Due Diligence

The Township may assess Vendor privacy and security practices before entering into an agreement or implementing a service.

Assessments may consider:

- sensitivity and volume of information involved;
- security safeguards;
- data storage and processing locations;
- subcontractor arrangements;
- incident response capabilities; and
- relevant certifications or independent assessments.

8.2 Privacy and Security Assessments

The Township may require a Privacy Impact Assessment (PIA) and/or other privacy, security, or technology assessments for services involving higher-risk information, new technologies, cloud services, artificial intelligence, automated processing, or significant changes to existing services.

Vendors shall provide information reasonably required to support such assessments.

8.3 Audit and Compliance Verification

The Township may conduct reasonable and proportionate compliance reviews to confirm Vendor adherence to contractual and policy requirements.

Oversight activities may include:

- review of relevant documentation;
- review of security certifications or assessments;
- verification of applicable controls; and
- review of records relating to Township information.

The Township shall exercise oversight in a manner that considers Vendor confidentiality, security requirements, and operational constraints. Where possible, the Township may rely on current third-party certifications, audit reports, or assessments provided by the Vendor.

8.4 Vendor Cooperation

Vendors shall cooperate with reasonable Township compliance reviews and address identified deficiencies within agreed timelines.

9. CLOUD SERVICES AND TECHNOLOGY PROVIDERS

9.1 General Requirements

Cloud service providers, SaaS providers, and technology Vendors shall ensure Township information is securely stored, processed, accessed, and protected.

Providers shall maintain:

- appropriate access controls;
- security monitoring and logging;
- system availability and reliability measures;
- backup and recovery capabilities; and
- processes supporting secure data export and transition.

9.2 DATA RESIDENCY AND CROSS-BORDER PROCESSING

The Township prefers that personal information be stored and processed within Canada where reasonably practicable.

Vendors shall disclose:

- locations where Township information is stored or processed;
- any cross-border data flows; and
- material changes to storage or processing locations.

9.3 Artificial Intelligence and Automated Processing

Vendors using artificial intelligence, machine learning, or automated processing involving Township information shall:

- disclose such use to the Township;
- protect Township information from unauthorized use or disclosure;
- not use Township information to train publicly available or shared models without written authorization; and
- provide reasonable information regarding how such technologies process Township information.

9.4 Business Continuity and Disaster Recovery

Technology Vendors shall maintain appropriate business continuity and disaster recovery measures to support the availability and recovery of Township information and services.

Where appropriate, Vendors shall periodically test recovery procedures and address identified deficiencies.

10. Records Lifecycle and Retention Requirements

10.1 Retention Requirements

Vendors shall manage Township information in accordance with applicable Township retention requirements and contractual obligations.

Where reasonably practicable, Vendor retention practices shall align with Township requirements.

10.2 Lifecycle Management

Vendors shall support the appropriate management of Township information throughout its lifecycle, including authorized use, retention, transfer, return, and disposal.

10.3 Backups and Replication

Vendors shall maintain reasonable controls for backup and replicated copies of Township information to support security, availability, and appropriate retention practices.

10.4 Legal Holds

Where the Township provides notice of a legal hold affecting Township information, Vendors shall take reasonable steps to preserve relevant information and suspend routine deletion processes as required.

10.5 Return and Disposal

Upon completion of services, termination of an agreement, or request by the Township, Vendors shall return or securely dispose of Township information in accordance with contractual requirements and applicable obligations.

Where appropriate, Vendors shall confirm completion of return or disposal activities.

11. COMMUNICATIONS AND SOCIAL MEDIA VENDORS

Vendors acting on behalf of the Township shall follow approved communications requirements, protect Township information, and promptly report any privacy, security, or communication incidents. Vendors shall not disclose personal information, confidential information, or represent personal opinions as official Township positions.

12. CONFIDENTIALITY

Vendors shall ensure that Township information is treated as confidential and accessed only by authorized individuals for approved purposes. Confidentiality obligations shall continue following completion or termination of services.

13. NON-COMPLIANCE

Failure to comply with this Standard or contractual obligations may result in corrective action, restriction of access, or other contractual remedies.

14. REVIEW

This Standard shall be reviewed periodically to ensure continued alignment with applicable privacy, security, records management, and technology practices.

15. EFFECTIVE DATE

This Policy comes into effect on the date approved by Council.

Information Asset Register Policy

1. PURPOSE

The purpose of this Policy is to establish a framework for identifying, documenting, maintaining, and reviewing the Township of Armour's Information Asset Register.

The Information Asset Register replaces the former Personal Information Bank (PIB) inventory maintained under previous legislative requirements. It is maintained as an internal governance and administrative tool to support the responsible management, protection, and oversight of information held by the Township.

The Register supports, but does not replace, the Township's obligations under applicable legislation and municipal policies.

2. SCOPE

This Policy applies to all Township departments, boards, committees, employees, contractors, consultants, volunteers, and agents acting on behalf of the Township.

It applies to information created, collected, received, used, or maintained by the Township in any format, including paper records, electronic files, databases, and information systems.

3. DEFINITIONS

For the purposes of this Policy:

"Information Asset" means information or a collection of information created, collected, received, or maintained by the Township to support its programs, services, and operations.

"Information Asset Register" means an internal record identifying the Township's information assets and documenting relevant information about their purpose, responsible department, location, protection, and retention.

"Personal Information" means recorded information about an identifiable individual, as defined by applicable legislation.

"Clerk/Privacy Officer" means the employee designated to coordinate the Township's information management, privacy, and access to information responsibilities.

4. LEGISLATIVE AUTHORITY

This Policy is established pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and shall be administered in accordance with applicable legislation,

regulations, municipal policies, records retention requirements, and guidance issued by the Information and Privacy Commissioner of Ontario.

Where legislation imposes more stringent privacy requirements, those requirements shall prevail.

5. RESPONSIBILITIES

5.1 Council

Council shall approve this Policy and any amendments.

5.2 Chief Administrative Officer

The Chief Administrative Officer shall oversee the implementation of this Policy and promote compliance throughout the organization.

5.3 Clerk/Privacy Officer

The Clerk/Privacy Officer shall:

a) coordinate the maintenance and review of the Register;
b) provide guidance to departments on information management and privacy requirements;
c) coordinate updates with Department Heads; and
d) recommend improvements and corrective actions where necessary.

5.4 Department Heads

Department Heads shall:

a) identify information assets within their departments;
b) provide accurate information for the Register;
c) notify the Clerk/Privacy Officer of new information assets or significant changes; and
d) ensure information is managed in accordance with applicable legislation and Township policies.

6. INFORMATION ASSET REGISTER

The Register may be maintained in an electronic database, spreadsheet, or other approved format. The Register shall be maintained separately from this Policy. The database and its entries do not form part of the Policy and may be updated as required without Council approval, provided the updates remain consistent with this Policy. The Register shall be reviewed at least annually and updated as necessary.

7. PRIVACY AND INFORMATION SECURITY

Departments shall ensure that information, particularly personal information, is collected, used, disclosed, stored, and protected in accordance with applicable legislation and Township policies.

Only information reasonably necessary for an authorized purpose shall be collected, and appropriate safeguards shall be used to protect information against unauthorized access, use, disclosure, loss, or destruction.

Where a new program, technology, or information system may create significant privacy or security risks, the Clerk/Privacy Officer may require an appropriate assessment before implementation.

8. RECORDS RETENTION AND DISPOSAL

Information assets shall be retained and disposed of in accordance with the Township's Records Retention By-law, applicable legislation, and other relevant requirements.

Inclusion in the Register does not independently authorize the destruction of records or establish a retention period.

9. REVIEW

This Policy shall be reviewed by the Clerk at least once during each term of Council or sooner where legislative, technological, or operational changes require review.

10. EFFECTIVE DATE

This policy comes into effect on the date approved by Council.