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.