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.