Policy Number: IT-6013

Department: Information Technology

Division: Corporate Services

Adoption Date: April 13, 2026

Authority: CR 123/2026

Scheduled for Review: Oct 1, 2030

Artificial Intelligence (AI) Policy

1. Policy Statement:

This Artificial Intelligence Policy (the "Policy") outlines principles, guidelines, and rules for the responsible use of AI by Members of Council, employees, contractors, and agents of The Corporation of the City of Windsor (the "City"). Emerging technologies, like AI, will be evaluated and adopted by the City in a manner consistent with its values, policies, corporate strategic direction, plans, and other applicable frameworks or departmental priorities.

Purpose:

To establish clear, responsible, and practical guidelines for the use of AI technologies within the City.

To enable innovation and efficiency while ensuring transparency, accountability, security, privacy, and compliance with applicable laws.

2. Scope:

2.1. This Policy applies to the City, including all departments, divisions, and agencies, as well as all Members of Council, employees, officials, and agents engaged to represent the City, including any Users authorized to exercise discretion on its behalf.

2.2. This Policy applies to all Users who access or use AI to perform, or assist in performing, any activities in the usual course of their employment on behalf of the City, or while acting as agent of the City, regardless of location or device.

2.3. This Policy covers all AI tools, systems, and services used to support City operations, decision-making, or service delivery, whether internally developed, procured externally, or embedded within third-party products.

3. Definitions:

3.1. "AI Advisory Committee": means cross-departmental advisory body established to provide guidance, expertise, and non-binding recommendations on the responsible, ethical, secure, and compliant use of AI within the City. The AI Advisory Committee supports informed decision-making by assessing risks, impacts, and best practices related to AI use.

3.2. "AI" or "Artificial Intelligence": means technology that enables machines or computational systems to perform tasks that typically require human intelligence. This definition encompasses all current and foreseeable future forms of AI, including:

3.2.1. Narrow or specialized AI (tools designed for specific tasks such as content generation, data analysis, prediction, automation, or pattern recognition);

3.2.2. Generative AI (systems that create new content, such as text, images, code, audio, or video, from user inputs);

3.2.3. Algorithmic or machine learning-based AI (systems that learn from data to make decisions or predictions); and

3.2.4. Any AI systems and tools that encompass current and foreseeable future capabilities.

In the context of the City, AI refers to any such technology used for municipal operations, public service delivery, productivity enhancement, citizen engagement, decision-support, or any other work-related activity, and is subject to the requirements of this Policy for responsible, ethical, secure, transparent, and accountable adoption. For greater certainty, this definition does not include basic automation or deterministic rule-based systems that do not involve learning, inference, or content generation.

3.3. "Council": means the council of the City.

3.4. "IT Governance Committee": means the corporate-level decision-making body composed of members of the Corporate Leadership Team and the Chief Administrative Officer, and chaired by the CIO. The IT Governance Committee is responsible for providing strategic oversight and decision-making authority over the City's IT projects and enhancements portfolio. The IT Governance Committee reviews, prioritizes, and approves IT initiatives based on strategic alignment, value, risk, resource availability, and budget constraints through a formal governance cycle.

3.5. "IT Governance Framework": means the IT Governance Framework as approved by the Chief Administrative Officer, as may be amended from time to time.

3.6. "Privacy": The protection of personal information under the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA") and personal health information under the *Personal Health Information Protection Act* ("PHIPA"), including the lawful collection, use, disclosure, retention, and disposal of such information, and ensuring it is safeguarded from unauthorized access, use, or disclosure.

3.7. "User": means any individual who accesses or uses the City's IT resources, systems, or AI tools in the performance of any activities in the ordinary course of their employment on behalf of the City, or while acting as agent of the City, including but not limited to, Members of Council, City employees, contractors, consultants, vendors, and representatives of any City department, division, or agency, and "Users" shall mean more than one of them.

4. Responsibilities:

4.1. The AI Advisory Committee, comprised of cross-departmental City employees, is responsible for providing advisory oversight, guidance, and non-binding recommendations related to the responsible use of AI systems and tools. All approvals for AI-related initiatives, projects, pilots, or implementations shall be governed through the City's IT Governance Framework, with decision-making authority resting with the IT Governance Committee, and executive oversight by the CIO. The AI Advisory Committee shall:

4.1.1. Conduct AI impact assessments to identify and evaluate legal, ethical, bias-related, privacy, security, operational, and reputational risks associated with proposed or existing AI use cases;
4.1.2. Periodically review approved AI tools and initiatives from an advisory and risk-informed perspective, providing guidance on lifecycle management, emerging risks, and best practices, without altering or superseding governance approvals; and
4.1.3. Where appropriate, provide advisory recommendations to the CIO, the IT Governance Committee, Corporate Leadership Team, or Council, regarding proposed AI uses or solutions for the implementation of new initiatives, projects, pilots, or departmental applications, including recommended mitigation measures and alignment considerations with City priorities, values, and applicable laws.

4.2. The Chief Information Officer/Executive Director of Information Technology (the "CIO") is responsible for approving the use of AI systems and tools, as well as monitoring and auditing their implementation and performance.

4.3. The Manager of Records/Elections & Freedom of Information Coordinator is responsible for evaluating the use of privacy impact assessments and Privacy concerns related to AI.

4.4. The Senior Manager, Cyber Security & Risk is responsible for ensuring appropriate Privacy, security and risk management controls are applied to all approved AI systems and tools, including ensuring that reasonable and proportionate logging and audit mechanisms, where available, are considered and leveraged to support security oversight, and that regular security assessments and vulnerability testing are conducted to identify, assess, and remediate security weaknesses or vulnerabilities in accordance with organizational information security risk management practices.

4.5. All **Users** are responsible for:

4.5.1. Understanding and complying with this Policy, protecting City data, including personal information as defined under the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA") and personal health information as defined under the *Personal Health Information Protection Act* ("PHIPA"), and obtaining required approvals prior to the use or implementation of AI systems or tools.

4.5.2. Reviewing and verifying all AI-generated or AI-assisted outputs for accuracy, completeness, fairness, and alignment with the City's core values before using them in any work product, decision, communication, or external publication. Outputs must be assessed for potential biases (especially in analysis, recommendations, or citizen-facing content), with appropriate mitigation, and must meet the same standards of accuracy, quality, and professionalism as non-AI work.

4.5.3. Complying with applicable laws, legislation, regulations, City by-laws, policies, procedures and standards, and ethical guidelines governing intellectual property, Privacy, data protection, and any other relevant areas.

4.5.4. Retaining sufficient documentation, in accordance with the City's records retention requirements, where AI is used to materially inform decisions, recommendations, or public-facing outputs, to support transparency, auditability, and accountability beyond the initial review and validation of AI-generated content.

4.5.5. Reporting immediately any suspected or confirmed security weaknesses, vulnerabilities, or incidents related to AI usage to the Chief Information Officer/Executive Director of Information Technology.

4.5.6. Committing to ongoing development of AI literacy, through attendance at City-provided training.

5. Policy:

Governing Rules and Regulations:

5.1. Guiding Principles: To maintain public trust and ensure the responsible development, deployment, and use of AI tools throughout the entire AI lifecycle, including decommissioning, the City will be guided by the following principles:

5.1.1. Fair: AI use will comply with all applicable laws, legislation, regulations, and City by-laws, policies, practices and standards, including those related to human rights, accessibility, and fairness obligations. The City will take reasonable steps to mitigate and remedy bias and ensure equitable outcomes in AI-assisted work and services.

5.1.2. Accountability: Clear accountability for AI use will be maintained through defined roles and responsibilities as outlined in this Policy. Approvals for AI development, deployment, and use will be obtained in accordance with this Policy.

5.1.3. Secure: AI infrastructure and tools will be appropriate for the security classification of the information involved. Privacy and personal information will be protected, and cybersecurity risks will be assessed and managed in accordance with City by-laws, policies, procedures and standards and applicable laws.

5.1.4. Transparent: Users will exercise transparency in their use of AI by identifying AI-generated or AI-assisted content where appropriate or where directed by the IT Governance Committee, in accordance with this Policy, professional judgment and the directives of any government body, Court or Tribunal.

5.1.5. Educated: Users will be supported in developing knowledge of AI tools' strengths, limitations, and responsible use through City-provided training and resources.

5.1.6. Relevant: AI use will support User and organizational needs and contribute to better outcomes for residents and the public. Environmental impacts will be considered when selecting tools, and appropriate tools will be chosen for the task (AI is not the best choice in every situation).

5.2. Approval Required: Any AI solution, service, tool, application, or integration not previously approved, or any use involving higher risk (e.g., processing personal or sensitive information, citizen-facing decisions), must be evaluated and authorized in accordance with Section 4 (Responsibility) and applicable approval processes.

5.3. Non-compliance: Any non-compliance with this Policy may constitute misconduct and will be addressed in accordance with applicable City policies, collective agreements (for unionized employees), the Employment Standards Act (for non-unionized

employees), Terms and Conditions of Employment and relevant laws. Depending on the nature and severity of the breach, this may result in disciplinary measures, up to and including termination of employment (for cause, where applicable), contract termination (for contractors/agents), or referral to law enforcement, as directed by the City Solicitor.

5.4. Suspected Misuse: Any AI, security incidents, or Privacy concerns must be reported immediately to the Manager of Records/Elections & Freedom of Information Coordinator, or designate, for appropriate review and response.

5.5. **Conflict:** If there is a conflict with this Policy or any other City by-law, policy, procedure or standard, Users must contact the CIO, or designate, and City Solicitor, or designate, for clarification, reconciliation and direction.

5.6. Acceptable Use:

5.6.1. Users may only use AI for the performance of activities in the normal course of their employment at the City, or while acting as agent of the City, in accordance with this Policy and applicable laws. AI use must support the City's values, productivity goals, public service delivery, and legal obligations (including Privacy, security, human rights, and accessibility requirements). Users must use only approved AI systems and tools or those otherwise authorized in accordance with this Policy.

5.6.2. Users may use approved AI tools for routine tasks such as drafting, editing, summarizing, data analysis, brainstorming, meeting notes, internal workflow support, or similar productivity activities, or those otherwise authorized in accordance with this Policy.

5.7. **Prohibited Use:**

5.7.1. Personal Accounts: Users are prohibited from inputting City data or personal information as defined in MFIPPA and PHIPA into any AI systems or tools on personal accounts.

5.7.2. Sensitive Information: Users are prohibited from inputting or allowing unapproved AI system or tools to access any City data or personal information as defined in MFIPPA and PHIPA that contains personal, sensitive, or confidential information without explicit approval from the CIO, or designate, and the City Solicitor, or designate.

5.7.3. Business Decisions: Users shall not use AI to make decisions that affect individuals' rights or access to services without human validation from individuals with relevant experience.

5.7.4. Compliance with Laws and Regulations: Any use of AI that is not compliant with applicable laws or City by-laws, policies, procedures or standards is strictly prohibited.

5.7.5. Intellectual Property Rights: Unauthorized use of copyrighted material or creation of content that infringes on the intellectual property rights of others is prohibited.

5.7.6. Fraud and Misrepresentation: Using AI to create, generate, or distribute content for the purpose of fraud, misrepresentation, impersonation, or deception, including deepfakes or content that misrepresents an individual, group, or City position is prohibited.

5.7.7. Unauthorized AI Integrations: Installing, integrating, or using unapproved Application Programming Interfaces (APIs), plug-ins, connectors, add-ons, or software related to AI systems on City devices, networks, or accounts, as this may compromise security or introduce unauthorized data flows is prohibited.

5.7.8. Discrimination and Harmful Content: Using AI outputs or tools in a manner that discriminates against individuals based on protected grounds under the *Human Rights Code* or that creates inappropriate, harmful, discriminatory, or hateful content is prohibited.

5.7.9. Unauthorized AI Detection Tools: Relying on unauthorized AI detection tools or similar third-party services to evaluate or monitor AI usage, unless explicitly approved by the CIO, or designate, is prohibited.

5.8. AI Issue Escalation and Mitigation:

5.8.1. In the event that an AI system or tool produces inaccurate outputs, hallucinations, or other unintended results, departments or Users must promptly report the issue to the Information Technology department at the City. The Information Technology department will provide guidance on evaluating the impact, determining next steps, and implementing appropriate mitigation measures.

5.8.2. Mitigation may include, but is not limited to:

5.8.2.1. Temporarily or permanently limiting, pausing or canceling the use of the AI system or tool for the affected process.

5.8.2.2. Adjusting prompts, workflows, or data inputs to reduce risk of recurrence.

5.8.2.3. Engaging or recommending human review or validation from individuals with relevant experience for outputs critical to operations or decision-making.

5.8.2.4. Escalating the issue to the Chief Administrative Officer, or any other relevant City department, office, or external party as may be needed to assess, mitigate, and resolve the impact. Escalation may include, but is not limited to, third-party services, legal, risk management, or external experts.
5.8.5.5. Documenting the incident, the assessment, and corrective actions to support ongoing learning and risk management.

5.9. Access and Security:

5.9.1. Authorized Access: Access to AI systems and tools shall be restricted to authorized Users and managed in accordance with the City's identity and access management practices.
5.9.2. Secure Configuration: AI systems and tools shall be securely configured in accordance with applicable security standards, best practices, and vendor recommendations, commensurate with their risk and intended use.
5.9.3. User Authentication: Strong authentication mechanisms, such as multi-factor authentication, shall be implemented where technically feasible, or enforced through enterprise identity and access management controls, for User access to AI systems and tools.

5.10. Ongoing Review and Reassessment of AI Tools:

5.10.1. Approved AI systems and tools shall be subject to periodic review and reassessment to ensure continued alignment with City objectives, risk tolerance, legal requirements, and evolving technology standards. Reassessment may be triggered anytime by the CIO, or significant changes to the AI model, functionality, intended use, data inputs, vendor terms, legislation, or the occurrence of a material incident or risk. Where appropriate, approvals may be time-limited, conditional, modified, or withdrawn in accordance with the IT Governance Framework to manage emerging risks and ensure responsible use over time.

5.11. Privacy and Confidentiality:

5.11.1. AI use must comply with all applicable Privacy legislation, including MFIPPA and PHIPA. Personal information as defined in MFIPPA and PHIPA, and confidential, or sensitive information shall not be entered into AI tools unless explicitly approved and appropriately safeguarded in accordance with the terms of this Policy.

5.12. Vendor and Third-Party AI Requirements:

5.12.1. Where AI functionality is provided through third-party products or services, such vendors shall comply with this Policy and applicable City requirements. In addition, vendors may be required, as determined by the City through governance and procurement processes, to disclose the presence and general nature of AI functionality, comply with AI-specific security and privacy controls, and adhere to restrictions on the use of City data, including limitations on secondary use or model training, where applicable.

5.13. Training and Awareness:

5.13.1. Education and Training: Where applicable and practicable, Users shall be provided by the City with appropriate guidance, education, or training on the responsible and secure use of AI, commensurate with their role and the nature of the AI system or tool, prior to or as part of being granted access.

5.13.2. Awareness Campaigns: The City shall promote awareness of responsible AI use through periodic communications, guidance materials, or other reasonable means.

6. Additional Legislative Authority:

6.1.1. Acceptable Use Policy

6.1.2. Information & Digital Protection Policy

6.1.3. Electronic Monitoring of Employees Procedure

6.1.4. Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (Ontario)

6.1.5. Workplace Harassment Procedure

7. Records and Attachments:

7.1. Documents generated as a result of this Policy and any related procedures will be maintained in accordance with the City's Record Retention By-law subject to any other policy and/or applicable law

7.2. Summary of Amendments

Version	Date	Section Amended	Description of Change	Approved By