Corporate Artificial Intelligence Policy

Policy Owner	Director, Information Technology & Transformation
Policy Approver(s)	Executive Management Team
Related Policies	Acceptable Use Policy Code of Conduct Policy Corporate Information Access & Privacy Policy Electronic Monitoring of Employees Policy Video Surveillance Policy
Related Procedures	Artificial Intelligence & Generative Artificial Intelligence Guidelines (in progress) Privacy Breach Report Privacy Impact Assessment
Storage Location	CKCentral
Effective Date	April 26, 2025
Next Review Date	April 2026

1. Purpose

The purpose of this policy is to establish expectations for responsible, ethical and appropriate use of Artificial Intelligence (AI) and Generative Artificial Intelligence (Gen AI) technology.

2. Scope

This policy applies to all staff whether employed in a permanent, temporary or contract capacity, including full-time, part-time, casual, casual, seasonal, temporary, government sponsored programs, and volunteers.

For the purposes of this policy, the term “staff” refers to all persons identified in the preceding paragraph and the term “Municipality” refers to the Municipality of Chatham-Kent, including the Chatham-Kent Public Utilities Commission (PUC), Chatham-Kent Public Library Board (CKPL), and the Chatham-Kent Board of Health. Chatham-Kent Police Services (CKPS) is out of scope.

3. Definitions

3.1. **Accountability:** the obligation of all staff to explain and take responsibility for the outcomes of the use of AI.

3.2. **Artificial Intelligence (AI):** A computer’s ability to mimic human tasks and decisions; functions that would otherwise require human intelligence to execute.

3.3. **Bias**: Supporting or opposing a thing, person, or group compared with another, in an unfair way. Biases can interfere with impartiality, be conscious or unconscious, and be institutionalized into policies, practices, systems, and structures.

3.4. **Confidential Information:** Information entrusted to the Municipality of Chatham-Kent to carry-out programs and services which is non-public. It also includes restricted, non-public business information such as personally identifiable information (PII), health information, financial information, intellectual property and proprietary information. If disclosed, it could cause harm and must be treated securely.

3.5. **Fairness**: Impartial and just treatment or behavior without favoritism or discrimination. AI reflects current social relations and contexts and therefore has the potential to reinforce biases, discrimination, and inequities.

3.6. **Generative Artificial Intelligence (GenAI):** A subfield of AI, generates or creates new content through natural language processing (NLP). GenAI created output can be a simple text response or complex, seemingly comprehensive, content. New content can be text, images, video, audio, software code, etc. Examples: Open AI's ChatGPT, Google's Gemini, Microsoft's CoPilot.

3.7. **Large Language Models (LLM)**: Used by GenAI, massive amounts of information and data are used in training models, making their ability understand and generate content human-like. For example, interpreting inferences from context and contextually relevant responses.

3.8. **Machine Learning (ML)**: Imitates how humans learn from data, primarily through estimating patterns to predict or classify results. Results continue to improve through training data sets and reinforcement.

3.9. **Privacy**: Protection of personal data from unauthorized access, ensuring individuals retain control over their personal information.

3.10. **Privacy Breach:** An incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with personal, health, financial, or proprietary information protection requirements.

3.11. **Transparency**: Source materials, decision making process, and use of AI is clear and understandable to staff and citizens.

4. Policy Statement

AI is a rapidly evolving and complex set of technologies, quickly becoming embedded into all areas of daily life, including business systems and software used by municipal governments. This policy assists the Municipality in leveraging AI for the public good and to enhance productivity and efficiency while mitigating potential risks, complying with applicable laws, and respecting privacy, confidentiality and data security.

One of the most rapidly evolving areas is GenAI. GenAI uses LLM to generate new output or content through natural language processing. LLM are dependent on "very large volumes of personal information or data sets that may not be properly protected and may not always be lawfully collected at source" (Information and Privacy Commissioner of Ontario, 2024). Lack of data protection, and therefore lack of data privacy, is a significant concern if sensitive, personal or confidential data becomes available to GenAI systems.

GenAI presents many opportunities for Municipal government operations, research, and decision-making. GenAI is excellent at summarizing vast amounts of information and highlighting key concepts or unique items. It can provide quick answers to any topic it is trained on, and therefore well placed to act as an automated assistant, chatbot, or provide brainstorming services. These are examples of AI helping people more effective in their work, which should in turn provide value to citizens through improvements in service.

5. Guiding Principles

5.1. **Ethical Use:** AI systems and tools should be designed and deployed in ways that are fair, non-discriminatory, and respect human rights. Ethical considerations must be integrated into every stage of AI development and use.

5.2. **Transparency:** The decision-making processes of AI systems must be explainable and understandable. Stakeholders should be informed about how AI is used and how decisions are made.

5.3. **Accountability:** Clear accountability for the outcomes of AI systems must be established. This includes defining roles and responsibilities for those involved in developing, deploying, and monitoring of AI systems and tools.

5.4. **Privacy and Security:** AI use must comply with all applicable data privacy laws and regulations. Data collected and used by AI systems must be protected from unauthorized access and breaches.

6. Procedures

6.1. Selection and Implementation of AI systems and tools

AI systems and tools will be implemented through the ITT Project Intake process, or at a minimum, a ticket with the ITT Service Desk. AI systems and tools will be implemented in coordination with the ITT Division.

A Security Risk Assessment (SRA) and Privacy Impact Assessment (PIA) will be conducted for all AI systems and tools.

Annual reviews of AI systems and tools will be conducted to reassess and confirm use cases for the AI system and tool, including updating any use cases that involve personally identifiable information.

6.2. Acceptable Use

AI will be used in accordance with the Municipality of Chatham-Kent Employee Code of Conduct.

AI assisted tools such as chatbots must be supervised in their work and must work from a standard and approved set of processes and information, just as traditional customer service would.

6.3. Accuracy and Reliability

The logic and sources used to produce results is not transparent to the AI user. When the information and data within an AI or GenAI system is inconsistent, incomplete, or incorrect, using the AI generated results indiscriminately can clearly lead to unfair outcomes and perpetuate bias amongst historically disadvantaged groups. (Information and Privacy Commissioner of Ontario, 2024)

Accountability for AI and GenAI created content and output rests with the user. As such, Municipal staff are responsible for reviewing for accuracy, bias, and inappropriate disclosure of confidential or private information.

GenAI created content and output must not be disclosed, circulated, or used in a final product without prior review by Municipal staff.

7. Prohibited & Unacceptable Use

7.1. Municipal staff's use of AI is expected to comply with all applicable laws, regulations, policies.

Collection, use, or disclosure of confidential or private information or data must not be in contravention of FIPPA, MFIPPA, and PHIPA, Corporate ITT Acceptable Use Policy, or any other data protection requirements.

7.2. Confidential or private information or data must not be entered into or used with AI, as there are no guarantees of privacy or confidentiality.

7.3. AI is not meant to replace human expertise or judgement; therefore, AI must not be used to make decisions or recommendations impacting a specific individual or organization. For example, AI should not be used in processes such as performance reviews.

7.4. AI will be used in accordance with the Municipality of Chatham-Kent Video Surveillance Policy and the Electronic Monitoring of Employees Policy.

7.5. Use of AI should consider the potential impact to the public, and should be avoided or constrained where there may be an impact on public trust and public safety.

7.6. Privacy incidents or breaches must be reported to Municipal Governance through the Privacy Breach Reporting process.

8. Non-Compliance

8.1. Allegations of misconduct and/or misuse of AI will be investigated and pending the severity of the allegations, the use of Municipal ITT technology, devices, and access may be temporarily or permanently revoked. Legal action according to applicable laws and contractual agreements, may also be undertaken depending on the issue. Failure to comply with this policy could lead to disciplinary action up to and including termination of employment.

8.2. Suspect activity or abuse should be reported to an immediate supervisor and the Chief Human Resources Officer (CHRO).

8.3. The Municipality reserves the right to inspect any and all ITT systems, such as, but not limited to email, messages or chats, internet traffic, and files stored in private areas of its network in order to assure compliance with the policy under proper ITT process and guidelines.

9. Relevant Legislation

9.1. **Freedom of Information Protection of Privacy Act (FIPPA):**
FIPPA identifies the requirement for institutions "to protect the privacy of individuals with respect to personal information about themselves held by institutions".

9.2. **Municipal Freedom of Information Protection of Privacy Act (MFIPPA):**

MFIPPA also identifies the requirement for institutions "to protect the privacy of individuals with respect to personal information about themselves held by institutions". MIFFPA defines "institution" as a municipality, as well as local boards, commissions, and authorities.

Once personal information has been collected by a municipality it is considered within that institution's "custody or under its control". MFIPPA provides clear-cut for use of personal information by institutions:

i. The person has "has identified that information in particular and consented to its use"

ii. The information is being used in a manner consistent with intent of the original collection

MFIPPA clearly states the permissible reasons of disclosure of personal information under the custody or control of municipalities: disclosure is only acceptable in situations where the person has consented to disclosure of their personal information and is consistent with the original intent.

9.3. **Personal Health Information Protection Act (PHIPA):**

PHIPA establishes "rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information". PHIPA includes responsibilities for the custodians of health information.

10. Out of Scope

Chatham-Kent Police Services (CKPS): FIPPA and MFIPPA have sections apply that specifically to law enforcement. The collection, care and disclosure of personal information in the course of the work undertaken by CKPS does differ from Municipality's non-law enforcement business areas.

Revision History

Version	Change	Author	Date of Change
1.0	Draft	Erica Hoppe	October 18, 2024
1.0	EMT Approved	Erica Hoppe	April 26, 2025

References

Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, s 1,. (n.d.). Retrieved 2024-03-28, from https://canlii.ca/t/5652d

Government of Ontario. (2023, 03 09). *Freedom of Information and Protection of Privacy Manual*. Retrieved from Government of Ontario: https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual

Information and Privacy Commissioner of Ontario. (2024). *Artificial Intelligence in the public sector: Building trust now and for the future.* Retrieved 03 14, 2024, from Office of the Information and Privacy Commissioner of Ontario: https://www.ipc.on.ca/artificial-intelligence-in-the-public-sector-building-trust-now-and-for-the-future/

Kaplan, S., & Ravanera, C. (2022, 04 07). *An equity lens on artificial intelligence.* Retrieved from Government of Canada, Social Sciences and Humanities Research Council: https://www.sshrc-crsh.gc.ca/society-societe/community-communite/ifca-iac/evidence_briefs-donnees_probantes/skills_work_digital_economy-competences_travail_economie_numerique/kaplan_ravanera-eng.aspx

Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56. (n.d.). Retrieved 2024-03-28, from https://canlii.ca/t/552l1

Personal Health Information Protection Act, 2004, SO 2004, c 3, Sch A. (n.d.). Retrieved 2024-11-22, from https://canlii.ca/t/569mr