BY-LAW NO. 540-2026

A BY-LAW TO ESTABLISH THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS

1. PREAMBLE

1.1 WHEREAS subsection 37(1)(a) of the Community Safety and Policing Act, 2019, S.O. 2019, c. 1, Sched. 1, as amended ("CSPA") provides that a Board shall provide adequate and effective policing in the area for which it has policing responsibility as required by Section 10 of the CSPA;

1.2 AND WHEREAS subsection 38(1)(a) and 38(2) of the CSPA provides that the Board shall establish policies respecting the administration of the police service and may establish policies respecting any other matters related to the police service;

1.3 AND WHEREAS the Information and Privacy Commissioner of Ontario (IPC) and the Ontario Human Rights Commission (OHRC) have released joint Principles to guide the responsible adoption of Artificial Intelligence (AI) systems;

1.4 AND WHEREAS the Ontario Public Service (OPS) has issued a Directive on the Responsible Use of Artificial Intelligence that sets out the requirements for the transparent, responsible and accountable use of AI;

1.5 AND WHEREAS the Board deems it expedient to pass a by-law to establish policies regarding the use of AI Technologies to ensure they are developed, acquired, used, and decommissioned in a manner that is responsible, transparent, and adhere to ethical standards, legal and regulatory requirements, and comply with relevant legal and regulatory frameworks, including, but not limited to, data privacy and security requirements.

NOW THEREFORE THE REGIONAL MUNICIPALITY OF NIAGARA POLICE SERVICE BOARD ENACTS AS FOLLOWS:

2. DEFINITIONS

2.1 *"Act" or "CSPA"* means the *Community Safety and Policing Act, 2019, S.O. 2019, c. 1, Sched. 1,* and amendments thereto.

2.2 *"Artificial Intelligence (AI) Systems"* refers to any machine-based system or integrated set of technologies, data, processes, and human interactions that use computational methods, including machine learning, statistical modeling, or rule-based logic, to generate outputs such as predictions, recommendations, content, or decisions that influence operational, administrative, or public-facing outcomes. AI Systems include all components across their lifecycle, including data collection, model development, deployment, use, monitoring, and decommissioning, whether developed internally or procured from third parties. For greater clarity, AI systems may operate at varying levels of autonomy, but within Niagara Regional

Police Service, they are to be used as decision-support tools and must not replace human judgment, professional discretion, or legal accountability. All AI-enabled outputs remain subject to human review, validation, and approval, in accordance with applicable laws, policies, and ethical standards.

2.3 *"Bias"* means incomplete, imbalanced or historically biased data, flawed algorithms, human use or unintended design choices, which may lead to systemic and unfair outcomes, such as discriminating against certain individuals or groups over another in ways that differ from the intended function of the algorithm, in the AI model outputs or decisions made.

2.4 *"Board"* means the Regional Municipality of Niagara Police Service Board.

2.5 *"Chief"* means the Chief of the Niagara Regional Police Service.

2.6 *"Human Rights AI Impact Assessment"* means a tool that provides organizations with a method to assess AI systems for compliance with human rights obligations. The purpose of this human rights AI impact assessment ("HRIA" or "the tool") is to assist developers and administrators of AI systems to identify, assess, minimize or avoid discrimination and uphold human rights obligations throughout the lifecycle of an AI system.

2.7 *"Lifecycle"* means the lifecycle of AI which includes the following stages: design, data and modelling; verification and validation; deployment; operation and monitoring; and decommissioning.

2.8 *"Privacy Impact Assessment"* means a process that reviews a new or existing information system or program to determine whether measures are necessary to ensure compliance with personal information protection requirements in statute and regulation and to address the broader privacy implications of the system or program.

2.9 "Service" means the Niagara Regional Police Service.

3 BOARD POLICY

3.1 The Board supports the responsible use of Artificial Intelligence (AI) Systems to enhance public safety, improve service delivery, and advance innovation. The Board is committed to ensuring that the adoption and use of AI Systems align with the principles of fairness, transparency, accountability, and protection of privacy.

The Board will provide governance oversight of the Niagara Regional Police Service (Service) deployment or enhancement of AI-enabled systems, particularly where such systems may present a moderate, high or critical risk of disproportionately impacting members of the community. In exercising this oversight, the Board will consider both the potential benefits of AI Systems and the need to safeguard the rights and well-being of individuals and communities.

The Board expects that any use of AI Systems will comply with the applicable Canadian and Ontario laws and regulatory requirements, including those related to privacy, human rights, and individual rights and freedoms. The Service shall ensure that the appropriate risk assessments, safeguards, and governance measures are in place, and that decisions regarding the adoption and use of AI Systems are informed by evidence-based practices, including stakeholder engagement where appropriate, to identify and mitigate potential impacts.

The Board may, where appropriate, require reporting, evaluation, or review of AI-enabled systems to support transparency, accountability, and continuous monitoring throughout the lifecycle of such systems.

4 GUIDING PRINCIPLES

4.1 The Board hereby adopts the following IPC-OHRC Principles and ensures they are adhered to when considering the adoption and use of AI Systems. These principles are to be considered interconnected and of equal importance.

4.1.1 Valid and Reliable: AI Systems must exhibit valid, reliable, and accurate outputs for the purpose(s) for which they are designed, used, or implemented.

4.1.2 Safe: AI must be developed, acquired, adopted, and governed to prevent harm or unintended harmful outcomes that infringe upon human rights, including the right to privacy and non-discrimination.

4.1.3 Privacy Protective: AI should be developed using a privacy by design approach. Developers, providers, or users of AI systems should take proactive measures to protect the privacy and security of personal information and support the right of access to information from the very outset.

4.1.4 Human Rights Affirming: Human rights are inalienable, and protections must be built into the design of AI systems and procedures. AI systems must prevent and remedy discrimination effectively and ensure that benefits from the use of AI are universal and free from discrimination.

4.1.5 Transparency and Explainability: The Service shall ensure that any AI Systems it develops, acquires, or deploys are implemented in a manner that is visible, understandable, traceable, and explainable supporting transparency, accountability and public trust.

4.1.6 Accountable: The Service shall implement a robust internal governance structure with clearly defined roles, responsibilities, and oversight procedures, including a human-in-the-loop approach, to ensure accountability throughout the entire lifecycle of their AI Systems.

5. DIRECTION TO CHIEF

5.1 PROCEDURES

The Chief of Police shall establish the necessary procedures and processes defining the acceptable use and limitations on the deployment of AI Systems use by the Service.

5.2 PROCEDURAL GUIDELINES

The Chief of Police shall ensure the following guidelines are adhered to when considering the adoption and use of AI Technology and that the IPC-OHRC Principles are adhered to when considering the adoption and use of AI Systems:

5.2.1 Transparency: In instances where the Service uses AI Systems which have an impact on decisions that affect members of the public, they must be given notice of such uses, unless full transparency may unduly impact the efficacy of investigative techniques or operations. In such cases, the Chief of Police will endeavour to make publicly available as much information about AI Systems as practicable, to assure the public of the reliability of the AI Systems and the justifiability of its use.

5.2.2 Accountability: All use of AI Systems must be transparent and subject to performance measurement against recognized industry standards, supported by a clear governance framework, that ensures those responsible remain accountable for the decisions they make, including those informed or influenced by AI Systems or other algorithmic tools.

5.2.3 Fairness: Use of AI Systems must not result in the increase or perpetuation of bias in policing and should seek to reduce the existence of such biases. The application of AI Systems in the delivery of police services must foster fairness by:

a) Ensuring equality and non-discrimination in AI operation;
b) Protecting vulnerable groups from potential biases or adverse impacts;
c) Promoting diversity and accessibility in AI development and use; and
d) Enabling the review and correction of AI-supported decisions.

5.2.4 Justifiability: The use of AI Systems must be shown to further the purpose of law enforcement in a manner that outweighs identified risks.

5.2.5 Legality: All AI Systems used, and all use of AI Systems, in the course of delivering police services, must comply with applicable law, including the Community Safety and Policing Act (and its regulations, and successor legislation), Ontario's Human Rights Code, Municipal Freedom of Information and Protection of Privacy Act, the Information and Privacy Commissioner of Ontario, the Canadian Charter of Rights and Freedoms, and be compatible with applicable due process and accountability obligations.

5.2.6 Public Engagement: Where appropriate and as contemplated by Subsection 5.3.2 (f) below, public engagement can be crucial in establishing that AI Systems are used responsibly and takes a measured approach to the risk, cost, and community impact in the use of AI Systems.

5.2.7 Privacy: Any use of AI Systems must protect personal and sensitive information that is collected, in accordance with Section 5.5.2 below, and must be proportionate and reasonable, and minimize potential risks and negative impacts.

5.2.8 Reliability: AI Systems must demonstrate reliable and repeatable behaviour, producing AI outputs or recommendations that are consistent, while ensuring that any risks from inaccurate results are carefully assessed and avoided in contexts where factual accuracy or data integrity is essential.

5.3 PROCUREMENT AND APPROVAL

The Chief of Police shall:

5.3.1 Ensure the appropriate industry standard risk assessment tools are incorporated into the review of AI Systems.

5.3.2 Conduct a risk assessment of the AI Systems, prior to the earlier of:

a) Seeking funds for the new AI Systems, including but not limited to applying for a grant, or accepting municipal, provincial or federal funds, or public or private in-kind or other donations;

b) Acquiring the new AI Systems, including acquiring such technology without the exchange of monies or other consideration;

c) Entering into agreements or where applicable, recommend the Board enter into agreements, to acquire, share, or otherwise use such AI Systems;

d) Not procure, utilize, or deploy a new AI Systems deemed to have a real risk of significant harm to the community, compromise the legitimacy of the Board or Service;

e) When reporting to the Board and seeking approval for the procurement and deployment of AI Systems with a moderate, high or critical risk classification the report will describe, at a minimum:

i. The operational need(s) the AI Systems will address, the intended use by the Service and how use of the AI Systems will improve on current practices or operations;
ii. Identify and where possible minimize the risk level assigned to the AI Systems, the rationale for the risk level assigned, and the rationale for continuing with the procurement, use or deployment despite the associated risk;
iii. The findings of a Privacy Impact Assessment and Human Rights AI Impact Assessment, and any risk analyses carried out in accordance with section 5.3.1 above, including any analyses required by the Information and Privacy Commissioner of Ontario and the legislative authority for the collection of personal information;
iv. How the AI Systems operates, the source of the training data, and evidence of the validity, accuracy and security of the AI Systems under consideration, based on industry standards;
v. An evaluation of the AI Systems vendor, including its record with regard to data security, privacy and ethical practices; and
vi. The estimated cost of acquiring and implementing the AI Systems.

f) Develop and implement a public engagement strategy for AI Systems with a moderate, high or critical risk classification, where appropriate, to transparently inform the public of the use of the AI Systems that collects data about members of the public or assists users in identifying, categorizing, prioritizing or otherwise making decisions pertaining to members of the public, prior to its deployment.

g) Once completed, the feedback received from consultations with relevant stakeholders and the general public will also be reported to the Board.

The Board shall:

h) Review the reports submitted in accordance with section 5.3.2(e) and may determine;

i. If additional analysis is required prior to approval of the procurement, deployment or use of the new AI Systems; and
ii. That the Service may initiate the procurement, deployment or use of the AI Systems, and identify any additional analysis, monitoring, auditing and reporting requirements beyond the ones required by this By-law that are to be imposed once use of the AI Systems commences.

5.4 DEPLOYMENT OF AI SYSTEMS

The Chief of Police shall:

5.4.1 Ensure the training of users of any AI Systems must address effective, legal, and ethical uses. Any follow-up training must be delivered to update the knowledge and skills of users as the AI Systems evolve.

5.4.2 Consult with the stakeholders and impacted communities to identify and address any concerns arising from the use of AI Systems which are categorized with a moderate, high or critical classification. The results of consultations will be reported to the Board, including any actions taken to mitigate the risks and the harms of the AI Systems.

5.4.3 Actively address and mitigate biases caused by the use of AI Systems to prevent discrimination against any community and ensure equitable outcomes.

5.4.4 Prohibit the use of any existing AI Systems that poses a serious risk or is harmful to the community.

5.5 DATA PRIVACY AND SECURITY

The Chief of Police shall:

5.5.1 Implement and maintain privacy and confidentiality procedures which shall include strict protocols for the collection, storage, access, and sharing of data to be used by or for AI Systems, adhering to privacy laws and regulations.

5.5.2 Ensure there are security measures to safeguard sensitive and personal information against unauthorized access and data breaches that will be caused by the improper use of AI Systems or any external cyber threats.

6 REPORT TO THE BOARD

6.1 To enhance accountability and transparency, the Chief of Police shall:

6.1.1 Maintain and regularly update a public registry of AI Systems used by the Service. The registry must outline the capabilities, limitations, data handling practices, and purposes of the used technologies.

6.1.2 Document the decision-making processes regarding the AI Systems including their selection, deployment, and use.

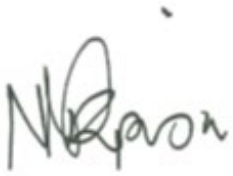
6.1.3 On an annual basis, and as may be additionally required by the Board, provide a public written report to the Board that demonstrates compliance with this By-law and an assessment of the achievements of the AI Systems according to the indicators established at the time the technologies were deployed. This report should include quantitative governance and performance indicators such as the AI Systems effectiveness; bias and fairness; compliance rates; data quality.

7 IMPLEMENTATION

7.1 This By-law shall come into force on the date of its passage.

ENACTED AND PASSED this 28th day of May, 2026.

THE REGIONAL MUNICIPALITY OF NIAGARA POLICE SERVICE BOARD



Nyarayi Kapisavanhu, Board Chair

Deb Reid, Chief Governance Officer