LPS-4-RT-002

Artificial Intelligence Technology Use

Policy Section 2: RT	Risk Management, Technology, Privacy, and Data Governance
Effective Date	April 16, 2026
Last Updated	April 2026
Approved By	London Police Service Board
Board Governance Policy Linkages	
Legislation	• *Community Safety and Policing Act, 2019* (CSPA) • *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) • *Ontario Human Rights Code* • *Canadian Charter of Rights and Freedoms*

1. Purpose

1. This Policy serves as the London Police Service Board's (the "Board") overarching Organizational Policy for Artificial Intelligence (AI) Technologies. Certain AI Technologies may warrant dedicated Board policies when their use is widespread, highly visible, or involves heightened considerations related to privacy, human rights, or public trust. In such cases, those policies operate in alignment with, and as a complement to, this Policy.
2. The purpose of this Policy is to establish the Board's expectations for the acquisition, assessment, deployment, and use of AI Technologies by the London Police Service (the "Service").
3. This Policy is intended to:
   a) Ensure that any AI Technologies used by the Service are lawful, ethical, fair, transparent, and accountable.
   b) Protect the rights, freedoms, and privacy of individuals and communities.
   c) Provide clear oversight expectations for the Board and clear direction to the Chief.
   d) Distinguish the Board's policy development and oversight role from the Chief's responsibility to develop and implement operational procedures and practices.
   e) Require that AI Technologies be assessed in a manner proportionate to their potential impact on rights, freedoms, safety, equity, and public trust before they are acquired, materially changed, or used.

2. Definitions

For the purpose of this Policy:

1. **AI Technology**: any system, software, application or device used in any division of the Service that uses automated or algorithmic techniques, including machine learning, neural networks, natural language processing, predictive technology or other statistical models, that analyzes data or generates outputs that are used to support, inform, or replace human decision-making about individuals, groups, or places.
2. **New AI Technology**: any of: (1) AI technology never used before by the Service, (2) goods and services, including but not limited to software and electronic devices, already or previously employed by the Service which are enhanced through the application of AI in a manner that transforms the goods or services into an AI technology; (3) AI technology already or previously employed by the Service which is being considered for deployment for a novel purpose or in novel circumstances that may substantially change the data collected or used, including the content of the data, its granularity, and the purpose of data collection and use; (4) AI technology already or previously employed by the Service which is being enhanced through the use of new data that is substantially different from the data previously used, including the type of data, its granularity, or the manner in which it is obtained; and, (5) the linking of data from existing sources of information to create a new dataset for use by an AI technology.
3. **AI Use:** deployment, operation, or reliance on outputs from AI Technology in any operational, investigative, administrative, or analytical function.
4. **Annual Artificial Intelligence Technology Compliance and Risk Report:** the annual report provided by the Chief to the Board respecting AI Technologies and other technologies with significant public impact, including their use, classification, governance controls, monitoring, audit findings, issues, and related trends.
5. **Bias**: systematically flawed output that is affected directly or indirectly by flaws in the design of the AI technology, training data, or the autonomous learning processes of the AI technology, to either misidentify certain types of subjects (individuals, objects, locations, etc.), or ascribe them with characteristics that disadvantage them based on illegitimate grounds (e.g., *Code*-protected grounds).
6. **Biometrics**: data on the measurements of physical and behavioural features of individuals (e.g., facial features, voice, gait) that could be used to identify the individual.
7. **Data**: any information collected and stored, whether locally or by a third party, which is used by the AI technology for training, validation, testing, or generating output.

8. **Explainability**: AI technology is explainable when human users can comprehend the results created by the machine, why they were arrived at, and how changes to the input would have changed the outputs.
9. **Human in the Loop**: a qualified human decision maker reviews and has genuine authority to accept, question, or reject AI outputs before any consequential decision is made.
10. **Risk Level:** the classification of an AI Technology according to its potential impact on rights, freedoms, safety, equity, and public trust, as follows:
    a) *Extreme Risk:* AI uses that present an unacceptable risk to rights or public trust, including severe and unmitigable bias, unjustified mass surveillance, or fully autonomous decision making in high-stakes contexts. These uses are prohibited.
    b) *High Risk:* AI uses that may significantly affect individual rights or freedoms, or that rely on sensitive personal data, biometric identification, or complex models whose errors may cause serious harm. These uses require Board approval and strict safeguards.
    c) *Moderate Risk:* AI uses that may affect individuals or groups but in a more limited or mitigated manner, or where the final decision remains subject to meaningful human review, yet errors or bias could still cause harm. These uses require Board approval and ongoing monitoring.
    d) *Low Risk:* AI uses that have limited impact on individuals or communities and are primarily administrative or supportive in nature, with minimal risk to rights and low potential for harm. These uses do not require Board approval but require notification to the Board.
    e) *Minimal Risk:* AI uses that have a negligible impact on individuals and are strictly internal or technical in nature. These may be managed through internal IT governance processes, but must still be inventoried where they qualify as AI Technology under this Policy.
11. **Training data**: data provided to the AI technology for the purpose of enabling it to learn patterns and independently develop decision-making algorithms.
12. **Transactional data**: data which is entered into a system which uses AI and that is used to generate output but is not leveraged for training.
13. **Vendor**: any external organization that develops, supplies, hosts, or maintains AI Technology for the Service.

Additional technical terms may be defined in Service procedures developed by the Chief, provided they are consistent with this Policy.

3. Legislative Authority and Context

The Board is responsible for the provision of adequate and effective policing in the City of London under s. 37(1)(a) of the *Community Safety and Policing Act, 2019*. This Policy is established in the context of the following legislative frameworks and oversight guidance:

1. ***Community Safety and Policing Act*, 2019 (*CSPA*):** Authorizes the London Police Service Board to set policies for the effective management of the London Police Service.
2. ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*:** Governs access, use, retention and disposal of recordings as personal information.
3. ***Ontario Human Rights Code:*** Prohibits discrimination in service delivery.
4. ***The Canadian Charter of Rights and Freedoms:*** Protects privacy and due process rights.
5. **Information and Privacy Commissioner of Ontario:** Provides guidance and recommendations to support compliance with provincial access and privacy legislation.

4. Scope

1. The Chief of Police (the "Chief") is responsible for the administration of the Service and shall comply with this Policy when authorizing or using AI Technologies.
2. This Policy applies to any AI Technologies that are:
   a) Developed, acquired, licensed, or used by the Service, directly or through a third party or vendor.
   b) Used to collect, process, analyze or generate information relating to members of the public, members of the Service, or communities, or to support, inform, or automate decisions that may affect individuals or groups.
3. This Policy applies to:
   a) New AI Technologies.
   b) New uses of existing technologies that introduce AI capabilities or change the risk profile.
   c) Use of existing technology that must be retrospectively classified to assess risk.
   d) Significant upgrades or vendor updates that add AI features to existing platforms.
4. This Policy applies across the lifecycle of AI Technologies, including procurement, assessment, deployment, use, monitoring, reassessment, and decommissioning.
5. This Policy does not apply to routine IT systems that do not involve algorithmic or automated decision making about individuals, such as basic word processing, email, or network infrastructure, unless those systems incorporate AI capabilities as described above.
6. Body-Worn Camera (BWC) Technology and related Digital Evidence Management Systems (DEMS) are governed under the Board's *Body-Worn Camera Policy LPS-4-RT-003.* To the extent that AI capabilities are incorporated into BWC systems or DEMS platforms, those features are also subject to this Policy's risk assessment and approval requirements.

5. Roles and Responsibilities

1. The Board is responsible for:
    a) Approving this Policy and any amendments.
    b) Considering and deciding on proposals for High and Moderate Risk AI Technologies.
    c) Receiving and reviewing the *Annual Artificial Intelligence Technology Compliance and Risk Report* on AI Use, risks, and impacts.
    d) Requesting reassessment of the Risk Level of any AI technology where the Board has reasonable grounds to believe the assigned Risk Level does not reflect the technology's actual impact or risk profile.
2. The Chief of Police is responsible for:
    a) Implementing this Policy.
    b) Classifying AI Technologies.
    c) Developing and implementing procedures, directives, and training.
    d) Ensuring that all AI use complies with legal, ethical, and policy requirements.
    e) Reporting to the Board as required under this Policy.
3. Sworn and Civilian members of the Police Service are responsible for complying with the Chief's procedures related to AI use.

6. Guiding Principles

All uses of AI Technologies, whether approved by the Board or otherwise, must adhere to the following guiding principles:

1. **Legality and Human Rights:** AI Technologies shall be used only in a manner that complies with the applicable laws, including the *Canadian Charter of Rights and Freedoms*, human rights legislation, privacy laws, and policing legislation.
2. **Fairness:** Use of AI technology must not result in the increase or perpetuation of bias in policing and should diminish such biases that exist. The Service shall take active, ongoing steps to identify, assess, and mitigate bias and discriminatory impacts arising from the use of AI.
3. **Justifiability:** The use of AI technology must be shown to further the purpose of law enforcement in a manner that outweighs identified risks.
4. **Organizational Accountability:** All use of AI technology must be auditable, transparent, and governed by a clear governance framework.

5. **Transparency:** The Service shall be as transparent as reasonably possible about the AI Technologies it uses, their purposes, and their impacts, subject to lawful limits related to operational security, ongoing investigations, or legal privilege. Where AI is used in a way that materially affects an individual or a case, such use should be appropriately and lawfully disclosed.
6. **Privacy:** Use of AI technology must, to the greatest degree practicable, preserve the privacy of the individuals whose information it collects in line with 'privacy by design' principles.
7. **Meaningful Engagement:** The adoption of specific AI Technologies shall be preceded by meaningful public engagement commensurate with the risks posed by the technology under consideration.

7. Policy Directives

7.1 Internal Standard Operating Procedures and Directives

1. The Chief shall establish and maintain clear Standard Operating Procedures and internal directives around the use of AI Technologies within the London Police Service, that at a minimum address:
    a) The designation and use of approved AI Technologies.
    b) The prohibition or controlled use of non-designated tools.
    c) The ethical and lawful application of AI.
    d) The protection of personal information.
    e) Ongoing risk assessment and monitoring.
    f) Training for members.
    g) Mechanisms for reporting material issues.
    h) Human in the Loop requirements.
    i) Requirements for reassessment when a Material Change occurs.

7.2 Identification and Risk Classification.

1. The Chief shall ensure that every AI technology is assessed and classified in accordance with the Risk Levels defined in section 2.10 of this Policy, using a structured risk assessment methodology that considers:
    a) The nature and sensitivity of the data involved.
    b) The rights, freedoms, and interests that may be affected.
    c) The likelihood and severity of potential harms, including bias and discriminatory impacts.
    d) The degree of human oversight and interpretability.
    e) The operational context in which the AI will be used.

2. The Chief shall ensure that any existing AI Technologies are re-assessed and re-classified in accordance with the Risk Levels defined in section 2.10 of this Policy using the above-listed methodology at any time that a vendor update to the AI technology introduces new AI capabilities.
3. Where the Board has reasonable grounds to believe that a classification does not accurately reflect the risk profile of an AI Technology, the Board may direct the Chief to reassess the Risk classification and report the results to the Board.
4. The Chief shall ensure that, for any new AI technology, any assessment and classification required under this section occur before the Service enters into a procurement commitment, executes a contract, materially expands use, or deploys the AI technology.

7.3 Prohibited AI Uses

1. The Service shall not develop, acquire, deploy, or use any AI Technologies that are classified as Extreme Risk as defined in section 2.10 of this Policy.
2. If any existing technology in use by the Service is found to meet the criteria for Extreme Risk, the Chief shall immediately discontinue its use and report this to the Board with a remediation plan.

7.4 Pre-Deployment Assessment and Board Approval

1. The Board retains approval authority for the deployment of AI Technologies classified as High or Moderate Risk.
2. Notwithstanding subsection 7.4.1, the Chair may exercise delegated approval authority where:
    a) The proposed deployment is time-sensitive and cannot reasonably await the next scheduled Board meeting.
    b) The circumstances require a decision to be made in the interest of operational continuity or risk management.
3. No AI Technologies classified as High or Moderate Risk shall be deployed unless approval has been granted by the Board, or by the Chair in accordance with 7.4.2.
4. Where the Chair exercises delegated authority under this section, the Chair shall report the decision, including the rationale and any conditions of approval, to the Board at the next available meeting.
5. When seeking approval of High or Moderate Risk AI Technologies, the Chief shall provide the Board in accordance with 7.4.1, or the Chair in accordance with 7.4.2, with:
    a) The risk classification and the rationale for the classification.
    b) Vendor information.
    c) The operational problem or need the AI is intended to address, and why AI is being considered.
    d) A plain language description of how the AI works and will be used, including data sources, data flows, and key outputs.

e) Any limitations or prohibitions.

f) Legal and privacy considerations.

g) Confirmation of compliance, or identified compliance risks, with the *Ontario Human Rights Code.*

h) The legal authority relied upon for any collection, use, or disclosure of personal information.

i) An assessment of potential bias or discriminatory impacts and proposed mitigation measures.

j) An assessment of impacts on disclosure obligations and Court scrutiny.

k) Any basic data governance items.

l) A summary of any consultations undertaken with regulators, Crown counsel, the community stakeholders, or experts.

m) Estimated costs and resource implications.

n) Proposed performance indicators for Board approval to evaluate whether the AI meets its intended goals and to detect adverse impacts.

6. AI Technologies classified as Minimal or Low Risk do not require prior Board approval.

7.5 Vendors and Third-Party Solutions

1. The Chief shall ensure that contracts and agreements with vendors that provide AI Technologies support compliance with this Policy and all other applicable policies of the Service, including but not limited to privacy, information security, procurement, and records retention.
2. Any vendor update or new capability that introduces AI functionality shall be reviewed and classified by the Chief before use.

7.6 Human Oversight

1. For all High Risk AI Technologies, the Chief shall ensure that a Human in the Loop assessment is conducted, such that no consequential decision affecting an individual is made solely based on AI output without meaningful human review and authorization.

7.7 Existing AI Technologies

1. The Chief shall review AI Technologies currently in use, classify each according to the Risk Levels in this Policy, and report the results to the Board in the annual *Artificial Intelligence Technology Compliance and Risk Report,* including the identification of any technologies that meet High or Moderate Risk thresholds.
2. Any existing AI Technologies determined to be Extreme Risk shall be immediately discontinued, and the Chief shall report to the Board on the steps taken and any associated impacts.

3. Any existing AI Technologies determined to be High or Moderate Risk may continue temporarily only in accordance with timelines and conditions set by the Board and are subject to the same approval, reporting, and monitoring requirements as new AI Technologies.

8. Public Disclosure, Reporting, and Accountability

8.1 Transparency and Public Engagement

1. The Service shall maintain a public-facing inventory of AI Technologies that are in use, subject to the exemptions outlined in 7.1.3 of this Policy:
   a) Identify each AI Technology by name.
   b) Describe its primary purpose and use in plain language.
2. For AI Technologies and other AI uses that may have a significant public impact, including those that affect large segments of the community, influence policing decisions affecting individuals, involve sensitive personal information, or raise notable privacy, civil liberties, or human rights considerations, the Chief shall develop a proportionate public engagement plan, which may include public information sessions, online consultations, or dialogue with relevant community groups and experts.
3. Disclosures in the public inventory may be limited at the Chief's discretion where release of information would compromise officer safety, investigative integrity, operational effectiveness, or where disclosure is restricted by law or investigative sensitivity.

8.2 Monitoring Moderate and High Risk AI Technologies

1. For each High or Moderate Risk AI Technologies approved by the Board, the Chief shall:
   a) Establish procedures and training requirements and cadence for members who will use or rely on these AI Technologies.
   b) Monitor the AI's performance and impacts using the performance indicators approved by the Board.
   c) Report to the Board within 12 months following the Board or Chair's approval of the AI Technology, through a dedicated post-implementation report separate from the annual *AI Technology Compliance and Risk Report,* on:
      i. How the AI Technology has been used in practice.
      ii. Its performance against expected outcomes.
      iii. Any privacy, legal, ethical, or operational issues encountered.
      iv. Any significant concerns raised by members of the Service, members of the public, or community stakeholders.

v. Any recommended changes, additional safeguards, or discontinuation.

2. Following the submission of the report referenced in subsection 8.2.1(c), the Board may determine the nature, frequency, and timing of any subsequent reporting requirements for the AI Technology to confirm that it remains necessary, effective, and appropriately classified.

8.3 Annual Artificial Intelligence Technology Compliance and Risk Report

1. The Chief shall provide the Board with an annual *Artificial Intelligence Technology Compliance and Risk Report* that addresses the Service's use of AI Technologies and other significant technologies with public impact, including Body-Worn Cameras and related DEMs.
2. The purpose of the annual *Artificial Intelligence Technology Compliance and Risk Report* is to support Board oversight of technology governance, legal compliance, public accountability, risk management, and continuous improvement.
3. The annual *Artificial Intelligence Technology Compliance and Risk* report shall include:
   a) An updated inventory of all AI Technologies in use and any changes in risk classification during the reporting period.
   b) A summary of any new AI Technologies in use and any changes in risk classification during the reporting period.
   c) Findings from any audits conducted during the reporting period, including key trends and risks.
   d) Notable updates on legal, compliance, or ethical matters.
   e) Any updates to vendor relationships or contracts with material AI or technology implications.
   f) BWC program reporting as required under the Board's *Body-Worn Camera Policy LPS-4-RT-003.*
4. Given the nature of the information captured within the *Artificial Intelligence Technology Compliance and Risk Report*, including system capabilities, vendor relationships, and identified risks, portions of the report may engage operational, legal, or security sensitivities.
5. Consistent with the provisions of the CSPA respecting Closed matters, reporting shall align with legislative expectations while balancing transparency and operational integrity.

8.4 Community Concerns and Statutory Complaint Processes

1. Recognizing the heightened public interest and potential impact associated with the use of AI Technologies, the Board shall provide a mechanism for members of the public to submit concerns related to the use of AI Technologies and may consider such concerns in its oversight of reports provided by the Chief under this Policy.
2. Nothing in this Policy alters the statutory complaint and oversight processes established under applicable legislation. Concerns or allegations relating to police conduct, service delivery, or compliance with legislative requirements shall be addressed through the appropriate process.