Kingston Police Service Board

Public Agenda Recommendation Report

To:	Chair and Members of the Kingston Police Service Board
From:	Policy and By-Law Committee
Subject:	Approval of Multiple Polices under the *Community Safety and Policing Act, 2019*
Date:	September 5, 2026

Strategic Priority Alignment:

Administrative/Procedural

Recommendation:

That the Kingston Police Service Board approve the policies listed in Report Number 26-71, as presented, in accordance with the *Community Safety and Policing Act, 2019*, and applicable regulations.

Background/Analysis:

The *Community Safety and Policing Act, 2019* (CSPA) establishes mandatory and discretionary policy responsibilities for police service boards. In support of the Board's governance role, the Kingston Police Service Board continues to review, update, and adopt policies to ensure alignment with legislative requirements, regulatory standards and applicable provincial guidance.

To streamline Board consideration, the following policies are presented as a consolidated package. These policies are administrative and governance-focused in nature and do not introduce substantive changes to the Board's strategic direction.

The following policies are submitted for the Board's approval:

- Anti-Corruption and Integrity Policy
- Information Technology and Information Security Policy

These policies have been developed and reviewed to ensure compliance with the *CSPA*, its regulations, and other applicable legislation, including but not limited to the *Occupational Health and Safety Act,* the *Accessibility for Ontarians with Disabilities Act,* and the *Municipal Freedom of Information and Protection of Privacy Act*, where applicable.

Financial Considerations:

The adoption of these policies does not result in additional financial implications for the Board. Any training, procedural or operational directives required to implement the policies fall within the responsibility of the Chief of Police and the Service's established management processes.

Contacts:

Gregory Ridge, Policy and By-Law Committee gridge@cityofkingston.ca

Wendy Stephen, Policy and By-Law Committee wstephen@cityofkingston.ca

Lorie Sargeant, Board Administrator 613-876-6984

Exhibits/Policies Attached:

- Exhibit "A" - Anti-Corruption and Integrity Policy
- Exhibit "B" - Information Technology and Information Security Policy

KINGSTON POLICE SERVICE BOARD

Anti-Corruption and Integrity Policy (GP-0XX)

Adopted:
Reviewed:
Revised:

Expires: Indefinite

Rescinds:

Legislation: Community Safety and Policing Act, 2019.

1. Policy Statement

The Kingston Police Service Board (the Board) recognizes the importance of effective screening, vetting, and supervision in preventing and detecting corruption and maintaining the integrity of the Kingston Police Service. The Board is committed to ensuring that appropriate measures are in place to identify and manage corruption risks throughout a member's career and to support effective supervision that identifies vulnerabilities, early warning signs of corruption, and performance deficiencies before they escalate or become systemic.

2. Definitions

For the purposes of this policy:

a) Corruption: conduct that involves the misuse or abuse of a police officer's or civilian member's position, authority, or responsibilities for an improper purpose or benefit, and that compromises, or has the potential to compromise, the integrity of policing.

b) Corruption risk: any circumstance, condition, behaviour, vulnerability, or other factor that creates or increases an opportunity for corruption to occur.

3. Board Policy

It is the policy of the Kingston Police Service Board, with respect to integrity and anti-corruption, that the Chief of Police will:

a) Ensure that appropriate screening and vetting practices are in place for police officers and civilian members:

   i. At the recruitment stage, to assess integrity, suitability, and the ability to meet Service standards; and

   ii. Throughout a member's career, including when progressing into more senior or high-risk roles, to identify and manage corruption risks and ensure continued suitability and ability to meet Service standards.

b) Ensure that supervisors are appropriately trained to identify:

   i. Areas of vulnerability;

   ii. Early warning signs of corruption; and

   iii. Performance deficiencies that may require intervention.

c) Ensure that consideration is given to how individual corruption risks may develop or contribute to systemic corruption within the Service and that appropriate measures are taken to identify and manage such risks.

d) Ensure that that screening, vetting, and supervisory practices are periodically reviewed and informed by relevant evidence and recognized practices from other jurisdictions and sectors, where appropriate.

_____ _____

Chair Board Administrator

KINGSTON POLICE SERVICE BOARD

Information Technology and Information Security Policy (AI-0XX)

Adopted:
Reviewed:
Revised:

Expires: Indefinite

Rescinds:

Legislation: Community Safety and Policing Act, 2019.

1. Policy Statement

The Kingston Police Service Board (the Board) recognizes the importance of maintaining a secure and reliable information technology environment to support the effective delivery of policing services and protect the confidentiality, integrity, and availability of police information and information systems. The Board is committed to ensuring that access to police databases and information systems is appropriately authorized, controlled, monitored, and protected against unauthorized access, misuse, and security threats.

2. Board Policy

It is the policy of the Kingston Police Service Board, with respect to information technology and information security, that the Chief of Police will:

a) Establish and maintain information technology and information security procedures appropriate to the Service's operational and organizational requirements and applicable legal and regulatory obligations.

b) Ensure that access to police databases and information systems is:

i. Authorized based on a member's role, responsibilities, and current duties;

ii. Limited in accordance with the principle of least privilege;

iii. Appropriately managed when a member's role, responsibilities, or duties change; and

iv. Revoked or otherwise appropriately restricted when access is no longer required.

c) Ensure that appropriate controls are established for the authorization, assignment, review, modification, and removal of access permissions to police databases and information systems.

d) Ensure that appropriate controls are established for privileged or elevated access to police databases and information systems.

e) Ensure that police databases and information systems are appropriately monitored to identify unauthorized or inappropriate access and activity.

f) Ensure that monitoring mechanisms support both:

i. Proactive identification of potential misuse and early warning signs of unauthorized or inappropriate activity; and

ii. Reactive review of access and system activity where potential misuse, unauthorized access, or a security incident is suspected or identified.

g) Ensure that confidential, sensitive, and police information is appropriately protected against unauthorized access, use, disclosure, loss, or destruction.

h) Ensure that safeguards are established to protect the Service's information technology environment against cybersecurity threats and unauthorized access.

i) Ensure that members are provided with appropriate information, training, and direction regarding their responsibilities for information security, including the appropriate use and protection of information technology resources and police information.

j) Ensure that procedures are established for members to promptly report suspected or confirmed information security incidents, including unauthorized access to or use of police databases and information systems.

k) Ensure that significant information security incidents, systemic concerns, or material risks are reported to the Board.

l) Ensure that the Service's information technology and information security framework is periodically reviewed and updated to address identified risks, changes to the Service's information technology environment, applicable legislative and regulatory requirements, and recognized practices.

_____ _____

Chair Board Administrator