



Policy Name:	Use of Artificial Intelligence		
Policy #:	AD 9.19.1	Last Updated:	08-26-2026
Issued By:	Corporate Services Bureau	Approved By:	ELT
Version:	1	Review Frequency:	AS REQUIRED

RELATED POLICIES

AD 9.18 Security and Confidentiality of Records and Information

AD 9.19 Information Technology (IT) Security

1. PURPOSE

- 1.1. The responsible use of Artificial Intelligence (AI) tools within Surrey Police Service (SPS) is essential to maintaining public trust, ensuring ethical conduct, and complying with applicable legal, regulatory, and information management requirements.
- 1.2. This policy establishes SPS's rules governing the use of AI tools, technologies, and techniques across the organization.

2. SCOPE

- 2.1. This policy applies to all SPS Employees (including Members and Civilian Staff), Volunteers, Practicum Students, and Contractors.

3. POLICY

- 3.1. Subject to approval and compliance with this policy, AI tools may be used for low-risk, non-sensitive, and non-evidentiary purposes, such as:
 - i. Administrative tasks and content drafting;
 - ii. Basic data analysis;
 - iii. Capturing and summarizing meeting notes;
 - iv. Developing reports and presentations; and
 - v. Drafting internal and external communications.

Responsibilities of All SPS Staff

- 3.2. All SPS staff are responsible for the following:

- i. Considering the risks, impacts, and ethical implications associated with the use of AI technologies;
- ii. Obtaining written approval from the Director, Information Management & Information Technology (IMIT), prior to using any AI tool, technology, or product that is not already approved by SPS;
- iii. Ensuring that the handling of SPS information used with AI tools complies with existing information management, privacy, and information technology policies and procedures; and
- iv. Supporting SPS efforts to monitor and manage AI-related risks throughout the lifecycle of AI tools, including intake, active use, and decommissioning.

Restrictions on Use

3.3. Employees must not use publicly available generative AI services, including free or paid consumer versions of ChatGPT, Claude, Gemini, Grok, Perplexity, Midjourney, DALL-E, or similar services, for SPS business purposes unless the service has been formally approved by SPS through the approval process. This includes creating free or paid AI accounts with SPS credentials, unless formally approved by SPS.

Approved and Valid Use of AI

3.4. Approval to use AI tools will only be granted through Director, Information Management & Technology (IMIT) and may require additional risk, privacy, and impact assessments.

3.5. When using an SPS-approved AI tool that operates in an environment not fully controlled by SPS (e.g., internet-based services or external data environments), Employees must comply with the following requirements:

- i. Information Handling Restrictions: do not enter sensitive, confidential, or personal information into AI tools unless explicitly authorized by SPS. This includes, but is not limited to:
 - a) Personally identifiable information (PII) or personal information as defined by the British Columbia *Freedom of Information and Protection of Privacy Act* (FOIPPA), including identification numbers, addresses, contact details, and financial information;
 - b) Passwords or authentication credentials; and
 - c) SPS-developed source code.
- ii. Sensitive or confidential SPS business information, including:
 - a) Investigative information or techniques;
 - b) Training materials;
 - c) Internal policies and procedures;
 - d) Internal business operations information; and
 - e) All other information that is Classified/Protected Data;
- iii. Employees must not submit information that could expose SPS to legal, regulatory, or reputational risk.

- iv. Critically assess, validate, and verify all AI-generated outputs before use. AI-generated content must not be treated as authoritative without independent review.
- 3.6. Where available, Employees should use opt-out features to prevent prompts or outputs from being used to train or improve AI models. SPS information must not become AI training data, knowingly or unknowingly. If opt-out options are unavailable or unclear, do not proceed and contact the IT Service Desk.
- 3.7. Employees should use discretion when using AI to verify information for accuracy, reliability and compliance with SPS policies. Employees must fact-check and amend any AI materials to ensure accuracy.
- 3.8. When AI-generated content is used in SPS work products, the AI tool name and version must be cited.
- 3.9. SPS-Managed AI Tools: Once SPS implements and manages approved AI tools internally, employees must adhere to policy requirements listed unless listed otherwise.

Risks of AI

- 3.10. The use of AI tools presents potential risks that all SPS Employees must understand:
 - i. **Hallucinations** - AI systems may produce inaccurate or misleading information. This risk is mitigated through careful verification and human oversight.
 - ii. **Bias and Discrimination** - AI outputs may reflect or amplify biases present in training data. This risk is mitigated through review, monitoring, and governance oversight.
 - iii. **Security Vulnerabilities** - AI systems may be targeted by cyber threats. Mitigation includes robust security controls and monitoring.
 - iv. **Ethical Concerns** - AI use may result in unintended ethical consequences. The SPS AI Working Group will review and assess proposed AI use cases.

Policy Enforcement

- 3.11. Failure to comply with this policy may result in operational delays, increased risk exposure, or inefficiencies. Repeated or significant violations may be escalated to senior leadership and may impact access to technology, systems, or funding approvals for application initiatives.

Exceptions

- 3.12. Any exceptions to this policy must be formally documented and approved by the IT Application Services Unit Manager, the Director of IMIT, and the Deputy Chief Constable, Corporate Services Bureau.

APPENDIX A: DEFINITIONS

“Artificial Intelligence (AI)” means a technological system that autonomously or semi-autonomously processes data related to human activities using techniques such as machine learning, neural networks, genetic algorithms, or similar methods to generate outputs including decisions, recommendations, predictions, or content.

“Classified/Protected Data” means data that is classified as:

- i. Protected A – Low Sensitivity: information that should not be disclosed to the public without authorization and could reasonably be expected to cause injury or harm.
- ii. Protected B – Particularly Sensitive: information that could cause severe injury or damage to the people or group involved if it was disclosed.
- iii. Protected C – Extremely Sensitive: information that, if compromised, could reasonably be expected to cause extremely grave injury, at less than the national interest level.

“Contractor” means a person or persons who have access to SPS premises or Electronic Communications System, as defined in this Policy, for the purpose of providing services or supplies to SPS on a contractual basis.

“Employee” means any employee of SPS (including Members and Civilian staff).

“Gen AI (GenAI)” means a subset of AI that generates new content (e.g., text, images, audio, code) based on patterns learned from large datasets and user-provided prompts. GenAI systems may simulate aspects of human learning and adapt outputs over time.

“GenAI Tools” means websites, software, or applications whether used through a web browser, mobile app, or desktop application that utilize Generative AI. ChatGPT, Microsoft Copilot, Midjourney, DALL-E are a few current examples of Generative AI systems.

“Machine Learning” means a branch of AI that enables systems to identify patterns in data and make predictions or decisions without explicit human-programmed rules

“Member” means a sworn Police Officer appointed by the Surrey Police Board.

“Practicum Students” mean students of a program at a recognized education institution who are engaged at a SPS premises for study, research, work experience, etc.

“Supervisor” means a Team Leader, Manager, Staff Sergeant, Sergeant, Inspector, Superintendent, Deputy Chief Constable, Chief Constable, and any other person acting in a supervisory capacity who is accountable for a particular area or shift on behalf of SPS.