POLICING PROJECT
NYU SCHOOL OF LAW

E: info@policingproject.org
W: policingproject.org

Police AI Policies

Ten Key Provisions to Include

As policing agencies begin to adopt a variety of artificial intelligence (AI) tools, it is crucial to establish safeguards that promote responsible use and ensure public trust. The ten provisions outlined in this document are designed to serve as baseline requirements for the governance of AI systems in the public safety context.

Although these provisions offer general guidance on the use of AI, additional policies may be necessary for certain specific tools. For example, agencies might have specialized policies relating to the use of face recognition technology or aerial drones. In developing such policies, agencies can build upon the general principles set forth here, tailoring them to the unique functions and uses of the AI system in question.

1. Scope

For purposes of this Policy, "AI" means a machine-based technology that can infer from the input it receives how to generate outputs, including content, decisions, predictions, or recommendations.

This Policy covers the Agency's use of AI tools (a) to investigate, detect, deter, or respond to criminal activity or other incidents affecting public safety, or (b) to create, or aid in the creation of, police reports or other investigative records. It does not cover AI

E: info@policingproject.org
W: policingproject.org

tools used for purely administrative tasks, such as scheduling or spelling or grammar correction.

> **Editor's Note.** This provision takes a "risk-based approach" to AI governance: it covers AI systems that pose a risk to individual rights or safety (such as tools used to investigate crime, uncover evidence, or generate official records) while excluding systems used for low-risk administrative functions. Examples of technologies that would be covered under this policy include face recognition technology, person-based predictive policing algorithms, automated license plate readers, and threat detection systems.

2. Chief AI Officer

The Agency shall designate a Chief AI Officer, whose responsibilities include:

A. Serving as a senior advisor to leadership regarding the agency's use of AI;

B. Overseeing compliance with this Policy by Agency personnel;

C. Ensuring processes are in place to evaluate AI systems before their deployment, including a review of any available evidence regarding their efficacy and potential impact on civil rights and civil liberties;

D. Ensuring Agency personnel receive appropriate training in use of AI systems, including verifying or corroborating system outputs if applicable;

E. Responding to grievances from individuals who believe they have been harmed by use of an AI system, and taking appropriate action; and

F. Managing personnel access to AI systems, including the authority to revoke access when this Policy is violated.

> **Editor's Note.** This section establishes the role of a "Chief AI Officer" to provide centralized oversight and ensure compliance. The provision is intended to be flexible: responsibilities may be assigned to an existing staff member or even shared among multiple staff members. Wherever possible, agencies should invest in helping their Chief AI Officer develop relevant expertise through training and professional development opportunities.

3. AI Inventory

On an annual basis, the Chief AI Officer shall publish an AI Inventory disclosing each AI system in use by the agency, including, for each system:

A. The vendor and product names (if applicable);

B. A brief description of the system's functions and capabilities;

C. A brief description of the data collected and/or analyzed by the system; and

D. The purposes for which use of the system is authorized.

> **Editor's Note.** AI inventories are an important tool to ensure transparency and accountability to the public. The inventory requirement in this model policy is intended to strike a balance, requiring agencies to disclose key details about what AI systems are used and for what reasons, while avoiding unnecessary technical disclosures that may prove burdensome for agencies to track and report.

E: info@policingproject.org
W: policingproject.org

4. Data Collection and Use

For each AI system that collects or analyzes personally identifiable information ("PII"), the Agency shall establish and document clear criteria specifying:

A. The individuals or categories of individuals whose PII is subject to collection and/or analysis; and

B. The conditions under which agency personal may access, query, or otherwise use data or system outputs containing PII, including whether a predicate is required, and what that predicate is.

> **Editor's Note.** This provision aims to prevent arbitrary or unjustified collection and use of personally identifiable information (PII) by AI systems. First, it requires agencies to define whose data is subject to collection — i.e., whether the system applies broadly to all individuals or targets a specific subset (and, if so, which subset). Second, it requires agencies to specify when personnel may access data — for example, whether a predicate such as reasonable suspicion or probable cause is needed before performing a query. This provision, though flexible, reinforces the principle that both data collection and use must be guided by clear, consistent standards.

5. Data Retention

For AI systems that collect or analyze PII, the Agency shall establish a data retention policy that specifies, for each such system, how long any collected or analyzed data may be retained. Subject to applicable law, this policy shall prescribe the shortest practicable retention period that is consistent with the agency's operational needs.

> **Editor's Note.** Agencies should retain only the minimum amount of data necessary to fulfill the intended purpose of an AI system. Limiting data retention helps reduce the risk of privacy intrusions, as the accumulation of data over time can reveal increasingly sensitive information about individuals. In addition, a limited retention period minimizes any harms from data breaches. Although it is difficult to prescribe a universal data retention period for all AI systems, agencies should establish a default timeframe and revisit it periodically in light of their experience, as well as emerging best practices.

6. Data Sharing

Before sharing data with another agency, the Chief AI Officer shall enter into a written data-sharing agreement with that agency. This agreement shall specify:

A. The data to be shared;
B. The purpose(s) of the sharing;
C. The duration for which the data may be retained;
D. Any limitations on the data's use.

In exigent circumstances involving a threat to life or serious bodily harm, data may be shared without a prior agreement, provided the Agency documents the disclosure and enters into a data-sharing agreement if any further data is to be shared with the recipient agency.

> **Editor's Note.** Data sharing can aid investigations, yet it also risks creating accountability gaps — for example, when data is used by a recipient agency for purposes not authorized by the sharing agency. This provision ensures that data sharing can occur, but only when subject to a clear, documented agreement defining the scope, purpose, and limits of such sharing.

E: info@policingproject.org
W: policingproject.org

7. Discriminatory Use Prohibited

No agency personnel shall use an AI system in a manner that targets an individual or group on the basis of:

A. Race, ethnicity, religion, or other protected characteristic, unless that characteristic is part of a specific suspect description; or

B. Express or perceived belief, absent a plausible basis to conclude that the individual or group is advocating conduct that poses a threat to public safety.

Any decision to target a particular geographic area for deployment of an AI system must be justified by a sound nondiscriminatory basis.

> **Editor's Note.** This section establishes two protections against discriminatory AI deployment: a prohibition on discriminatory targeting of an individual or group, and geographic deployment standards requiring evidence-based justification for targeting a particular area.

8. Disclosure of AI Use

When the Agency has used one or more AI systems within the scope of Section 1 in an investigation that results in a prosecution, such use shall be disclosed in a police report to be included in the casefile submitted to the prosecutor. This report shall include, at a minimum:

A. The name of the AI system; and

B. A brief description of the AI system's role in the investigation, such as whether it was used to generate an

investigative lead, detect unlawful activity, or corroborate evidence.

> **Editor's Note.** Often, the fact that police have used an AI system will not be apparent to prosecutors or defense counsel, especially when a system is used to generate leads (as opposed to evidence for trial). A failure to disclose the use of AI potentially can undermine the ability of counsel fully to mount an effective defense. This provision requires police to file a report disclosing AI use, so that prosecutors have the information necessary to meet their disclosure obligations under *Brady v. Maryland* and their state's discovery laws.

9. Generative AI for Reports/Records

A police report or other investigative law enforcement record that was created in whole or in part through use of any AI system that generates content (known as "Generative AI") shall include:

A. A disclaimer that the report or record contains content generated by artificial intelligence; and

B. A certification by the individual submitting the report or record that they have reviewed it for accuracy.

> **Editor's Note.** Some jurisdictions are piloting the use of AI systems capable of generating content to draft documents such as police reports. These generative AI tools may well provide productivity benefits for agencies, yet they also risk introducing errors into the record — which may prove relevant in trials, plea negotiations, or other proceedings. Accordingly, this provision requires disclosure in any report or other investigative law enforcement record in which generative AI has been used.

E: info@policingproject.org
W: policingproject.org

10. Auditing and Enforcement

On an annual basis, the Chief AI Officer or their designee shall conduct an audit of AI system logs to ensure compliance with this policy. Any access, use, or dissemination of an AI system or data derived therefrom in violation of this Policy will be referred to the Office of Internal Affairs [or the head of the Agency], and may result in sanctions including, but not limited to, suspension or termination.

> **Editor's Note.** Auditing is a fundamental component of sound AI governance, ensuring accountability and adherence to policies. Modern AI systems typically generate audit trails capturing user activities, system operations, and outputs. These logs should be reviewed at regular intervals to detect any system use not in compliance with the agency's policy or applicable laws.