AUDIO-ONLY RECORDING DEVICES, OVERT: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that overt audio-only recording devices do not use artificial intelligence and machine learning.	Public comments highlighted a lack of industry-standard definitions for artificial intelligence and machine learning.
Expanded upon overt audio-only recording device capabilities.	Added language clarifying overt audio-only recording device capabilities.
Expanded upon overt audio-only recording device rules of use.	Added language clarifying overt audio-only recording device rules of use.
Expanded upon overt audio-only recording device safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to overt audio-only recording devices when job duties no longer require access.
Expanded upon overt audio-only recording device data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon overt audio-only record device external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

AUDIO-ONLY RECORDING DEVICES, OVERT REVISION

Date of Revision	Description of Revision
February 4, 2026	This impact and use policy was revised to comply with the recently passed amendment to the POST Act under Local Law 56 of 2025.

ABSTRACT

The New York City Police Department (NYPD) uses overt audio-only recording devices to create objective real-time acoustic recordings, to develop investigations, and enhance personnel training.

The NYPD produced this impact and use policy because overt audio-only recording devices are capable of recording acoustic data, including conversations, occurring within the range of the device which allows the acoustic data to be retained by NYPD investigators.

CAPABILITIES OF THE TECHNOLOGY

Overt audio-only recording devices are pieces of acoustic (i.e., sound) data recording equipment; the mechanics of the device are housed in such a way that the device is not hidden, concealed, or disguised. Overt audio-only recording devices use a microphone to record any auditory signal that occurs within the devices' recording range, such as voices, conversations, gunshots, music, etc. NYPD personnel use overt audio-only recording devices to create contemporaneous, objective acoustic recordings. Personal use of this technology is prohibited.

NYPD investigators conspicuously operate overt audio-only recording devices in situations where undercover officer or informant safety is not an issue. For example, an overt audio-recording device may be placed on a table where an interviewee is seated prior to taking a recorded statement.

Overt audio-only recording devices used by the NYPD are manufactured by Panasonic, Olympus, and Sony. None of the NYPD overt audio-only recording devices are imbedded with real-time audio transmission capabilities or any kind of editing features. The devices cannot be used to change an audio recording, nor do they use any biometric measuring technologies

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

Overt audio-only recording device must be used in a manner consistent with the requirements and protection of the Constitution of the United States, the New York State Constitution, and applicable statutory authorities.

Overt audio-only recording devices may only be used by NYPD personnel for legitimate law enforcement purposes or other official business of the NYPD. Supervisory personnel responsible for oversight must authorize the use. The underlying facts are considered on a case-by-case basis prior to the utilization of the technology, including the legitimate law enforcement purpose to utilize the technology in a given circumstance.

Court Authorization: Penal Law Sections 250.00 and 250.05 make New York a one-party consent recording state. A conversation between two or more individuals may be legally recorded if at least one of the parties consents to being recorded. Court authorization is not necessary in order for the NYPD to use overt audio-only recording devices because a member of the NYPD consents and participates in the conversation where the devices are utilized.

Additional Guidelines: If necessary, the Intelligence Division will determine the need for overt audio-only recording devices for NYPD investigations involving political activity. The Intelligence Division is the sole entity in the NYPD that may conduct investigations involving political activity pursuant to the Revised *Handschu* Guidelines.

As with all NYPD operations, no person will be the subject of police action because of actual or perceived race, color, religion or creed, age, national origin, alienage, citizenship status, gender (including gender identity), sexual orientation, disability, marital status, partnership status, military status, or political affiliation or beliefs.

The misuse of overt audio-only recording devices will subject employees to administrative and potentially criminal penalties.

Addendum Obligation: In accordance with the Public Oversight of Surveillance Technology Act, an addendum to this impact and use policy will be prepared as necessary to describe any additional uses of overt audio-only recording devices.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Physical Safeguards & Security Measures: Overt audio-only recording devices are securely stored in NYPD facilities when not in use, in a location that is inaccessible to the public. Additionally, a supervisor must periodically inspect and account for the devices. Access to overt audio-only recording devices is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to the overt audio-only recording devices is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

Data Safeguards & Security Measures: Recordings obtained from overt audio-only recording devices are retained locally, either within a memory card inserted into the device or to the device itself. Relevant recordings may be downloaded and retained within the NYPD case management system. Only authorized users have access to these recordings. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to case management and computer systems is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty. Authorized users can only access data and perform tasks allocated to them by the system administrator according to their role.

The NYPD has a multifaceted approach to secure data and user accessibility within NYPD systems. The NYPD maintains an enterprise architecture (EA) program, which includes an architecture review process to determine system and security requirements on a case by case basis. System security is one of many pillars incorporated into the EA process. Additionally, all NYPD computer systems are managed by a user permission hierarchy based on rank and role via Active Directory (AD) authentication. Passwords are never stored locally; user authentication is stored within the AD. The AD is managed by a Lightweight Directory Access Protocol (LDAP) to restrict/allow port access. Accessing NYPD computer systems remotely requires dual factor authentication. All data within NYPD computer systems is encrypted both in transit and at rest via Secure Socket Layer (SSL)/Transport Layer Security (TLS) certifications which follow industry best practices.

NYPD personnel must abide by security terms and conditions associated with computer and case management systems of the NYPD, including those governing user passwords and logon

procedures. NYPD personnel must maintain confidentiality of information accessed, created, received, disclosed or otherwise maintained during the course of duty and may only disclose information to others, including other members of the NYPD, only as required in the execution of lawful duty.

NYPD personnel are responsible for preventing third parties from unauthorized access to information. Failure to adhere to confidentiality policies may subject NYPD personnel to disciplinary and/or criminal action. NYPD personnel must confirm the identity and affiliation of individuals requesting information from the NYPD and determine that the release of information is lawful prior to disclosure.

Unauthorized access of any system will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO RETENTION, ACCESS & USE OF THE DATA

Recordings obtained by NYPD overt audio-only recording devices may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigations, and disciplinary proceedings. Recordings are retained locally, either within a memory card inserted into the device or to the device itself. Once the memory capacity of the overt audio-only recording device reaches maximum capacity, the device stops recording. The device cannot continue recording until the memory is cleared.

Relevant recordings may be downloaded from the device, uploaded into an appropriate NYPD computer or case management system, and deleted from the device. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management is limited to personnel who have an articulable need to access the system in furtherance of lawful duty. Access rights within NYPD case management and computer systems are further limited based on lawful duty.

The NYPD retains and disposes of records pursuant to New York City Charter § 1133(f), (g) and (h). Pursuant to these provisions, the NYPD developed a retention schedule that was approved by the New York City Law Department and Department of Records and Information Services. This retention schedule governs the retention and disposition of NYPD records, and the NYPD retains and disposes of records pursuant to this schedule. The retention period of a "case investigation record" depends on its classification and is based on the final disposition of the case, i.e., what the arrestee is convicted of or pleads to. Further, case investigations are not considered closed unless they result in: prosecution and appeals are exhausted, a settlement, no arrest, or when restitution is no longer sought.

The misuse of any recording will subject employees to administrative and potentially criminal penalties.

POLICIES & PROCEDURES RELATING TO PUBLIC ACCESS OR USE OF THE DATA

Members of the public may request data collected by the NYPD through its use of overt audio-only recording devices pursuant to New York State Freedom of Information Law. The NYPD will review and evaluate such requests in accordance with applicable provisions of the law.

EXTERNAL ENTITIES

Entities outside of the NYPD do not have direct access to the information and data collected by overt audio-only recording devices.

If an overt audio-only recording device obtains a recording relevant to a criminal case, the NYPD will turn the recording over to the prosecutor with jurisdiction over the matter. Prosecutors will provide the recording to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request recordings contained in NYPD computer or case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the recording or information related to it to partnering law enforcement and city agencies pursuant to on-going criminal investigations, civil litigation, and disciplinary proceedings. Information is not shared in furtherance of immigration enforcement.

Following the laws of the State and City of New York, as well as NYPD policy, the recording or information related to it may be provided to community leaders, civic organizations and the news media in order to further an investigation, create awareness of an unusual incident, or address a community concern.

Pursuant to NYPD policy and local law, NYPD personnel may disclose identifying information externally only if:

1. Such disclosure has been authorized in writing by the individual to whom such information pertains to, or if such individual is a minor or is otherwise not legally competent, by such individual's parent or legal guardian and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
2. Such disclosure is required by law and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
3. Such disclosure furthers the purpose or mission of the NYPD and has been approved in writing by the Agency Privacy Officer assigned to the Legal Bureau;
4. Such disclosure has been pre-approved as in the best interests of the City by the City Chief Privacy Officer;
5. Such disclosure has been designated as routine by the Agency Privacy Officer assigned to the Legal Bureau;
6. Such disclosure is in connection with an investigation of a crime that has been committed or credible information about an attempted or impending crime; or
7. Such disclosure is in connection with an open investigation by a City agency concerning the welfare of a minor or an individual who is otherwise not legally competent.

Vendors & Contractors: The NYPD purchases overt audio-only recording devices and associated equipment or software from approved vendors. The NYPD emphasizes the importance of and

engages with vendors and contractors to maintain the confidentiality, availability, and integrity of NYPD technology systems.

Vendors and contractors may have access to NYPD overt audio-only recording devices associated software or data in the performance of contractual duties to the NYPD. Such duties are typically technical or proprietary in nature (e.g., maintenance or failure mitigation). In providing vendors and contractors access to equipment and computer systems, the NYPD follows the principle of least privilege. Vendors and contractors are only allowed access on a "need to know basis" to fulfill contractual obligations and/or agreements.

Vendors and contractors providing equipment and services to the NYPD undergo vendor responsibility determination and integrity reviews. Vendors and contractors providing sensitive equipment and services to the NYPD also undergo background checks.

Vendors and contractors are legally obligated by contracts and/or agreements to maintain the confidentiality of NYPD data and information. Vendors and contractors are subject to criminal and civil penalties for unauthorized use or disclosure of NYPD data or information.

If recordings obtained using NYPD overt audio-only recording devices are disclosed in a manner violating the local Identifying Information Law, the NYPD Agency Privacy Officer, upon becoming aware, must report the disclosure to the NYC Chief Privacy Officer within 24 hours. The NYPD must make reasonable efforts to notify individuals affected by the disclosure in writing when there is potential risk of harm to the individual, when the NYPD determines in consultation with the NYC Chief Privacy Officer and the Law Department that notification should occur, or when legally required to do so by law or regulation. In accordance with the Identifying Information Law, the NYC Chief Privacy Officer submits a quarterly report containing an anonymized compilation or summary of such disclosures by City agencies, including those reported by the NYPD, to the Speaker of the Council and makes the report publicly available online.

TRAINING

NYPD personnel utilizing overt audio-only recording devices receive command-level training on the proper operation of the technology and the associated equipment. NYPD personnel must use overt audio-only recording devices in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The use of an overt audio-only recording device, including the reasons for its use, must be discussed with a supervisor. Supervisors of personnel utilizing audio-only recording devices are responsible for security and proper utilization of the technology and associated equipment. Supervisors are directed to inspect all areas containing NYPD computer systems at least once each tour and ensure that all systems are being used within NYPD guidelines.

NYPD personnel are advised that NYPD computer systems and equipment are intended for the purposes of conducting official business. The misuse of any system or equipment will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

Integrity Control Officers (ICOs) within each Command are responsible for maintaining the security and integrity of all recorded media in the possession of the NYPD. ICOs must ensure all authorized users of NYPD computer systems in their command understand and comply with computer security guidelines, frequently observe all areas with computer equipment, and ensure security guidelines are complied with, as well as investigating any circumstances or conditions which may indicate abuse of the computer systems.

Requests for focused audits of computer activity from IAB, Commanding Officers, ICOs, Investigations Units, and others, may be made to the Information Technology Bureau.

HEALTH & SAFETY REPORTING

There are no known tests or reports regarding the health and safety effects of overt audio-only recording devices. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or public academic research regarding physical safety hazards have been identified pertaining to the use of overt audio-only recording devices or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that overt audio-only recording devices are used effectively and responsibly. The NYPD does not believe that this technology is being used in a manner that disparately impacts any protected groups as defined in the New York City Human Rights Law.

The safeguards and audit protocols built into this impact and use policy for overt audio-only recording devices mitigate the risk of partial and biased law enforcement. NYPD overt audio-only recording devices record real time acoustic information occurring in close proximity to the device. These devices are only utilized for investigative purposes under supervisory review. Access is restricted to authorized personnel. Overt audio-only recording devices do not use any biometric measurement technologies. Based on these safeguards, any theoretical risks of overt audio-only recording devices disparately impacting protected groups are effectively mitigated.

The NYPD is committed to the impartial enforcement of the law and to the protection of constitutional rights. The NYPD prohibits the use of racial and bias-based profiling in law enforcement actions, which must be based on standards required by the Fourth and Fourteenth Amendments of the U.S. Constitution, Sections 11 and 12 of Article I of the New York State Constitution, Section 14-151 of the New York City Administrative Code, and other applicable laws.

Race, color, ethnicity, or national origin may not be used as a motivating factor for initiating police enforcement action. Should an officer initiate enforcement action against a person, motivated even in part by a person's actual or perceived race, color, ethnicity, or national origin, that enforcement action violates NYPD policy unless the officer's decision is based on a specific and reliable suspect description that includes not only race, age, and gender, but other identifying characteristics or information.