VEHICLE MOUNTED CAMERAS: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that vehicle mounted cameras 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 vehicle mounted cameras capabilities.	Added language describing how vehicle mounted cameras compliments other NYPD technologies.
Expanded upon rules of use.	Added language clarifying vehicle mounted cameras rules of use.
Expanded upon vehicle mounted cameras safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to the technology when job duties no longer require access.
Expanded upon vehicle mounted camera data retention.	Added language to reflect NYPD obligations under federal, state and local record retention laws.
Expanded upon vehicle mounted camera external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Minor grammar changes.	Minor syntax edits were made.

VEHICLE MOUNTED CAMERAS 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, Local Law 56 of 2025.

ABSTRACT

The New York City Police Department (NYPD) uses vehicle mounted cameras throughout the NYPD's fleet of motor vehicles. Vehicle mounted cameras support public and officer safety and are used to contemporaneously create an objective recording of law enforcement encounters, provide archived videos for investigations and criminal prosecutions, improve training techniques, foster accountability, and encourage lawful and respectful interactions between the public and the police.

The NYPD produced this impact and use policy because vehicle mounted cameras can capture images of people, vehicles, locations, license plates, any other visual information, and any acoustic data that occurs within range of the device, and share the data with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

Vehicle mounted cameras are video recording devices connected to NYPD vehicles for the purpose of creating a real-time objective record of law enforcement encounters and NYPD trainings.

The NYPD uses 3 kinds of vehicle mounted cameras:

1. Dashboard Cameras ("dash-cams");
2. Rear Interior Facing Cameras; and
3. Watercraft Cameras.

Vehicle mounted cameras used by the NYPD are manufactured by Black Vue, Falcon, Panasonic, and Axon. NYPD dash-cams are installed on the front windshield of both marked and unmarked NYPD vehicles. They can record both video and audio of what occurs in front of the vehicle. Rear interior facing cameras memorialize what occurs within the passenger cabin of a NYPD vehicle during transport of an arrestee.

The current Axon systems (dash-cams and rear-facing interior cameras) record both audio and video when activated, and re-write over recorded video in 60 second intervals with no audio when not activated but powered on. When the dash-cam or rear-facing interior camera is activated via the "Event Button," automatic activation signal, or via the vehicle tablet, the dash-cam and/or rear-facing interior camera will then record audio and video until the recording is manually deactivated via the "Event Button" or vehicle tablet. The dash-cam and rear interior facing cameras will then return to the buffering state, and the process is repeated. Completed recordings encompass the 60 second pre-event buffer period up to the moment of manual deactivation. Recordings cannot be paused or muted, only stopped.

Watercraft cameras are mounted to several NYPD watercraft used by the Harbor Unit. These watercraft cameras were installed by the boat builders on their 45', 60', and 70' launches The cameras do not currently record, but rather act as a live camera while the launch is underway of what occurs on the deck or in front of the watercraft. Watercraft cameras do not record any acoustic data. Since the introduction of the NYPD's body-worn cameras (BWC),[1] using watercraft cameras to record launches is no longer necessary, as the BWCs provide much clearer video and audio.

[1] For additional information on body-worn cameras, please refer to the body-worn cameras' impact and use policy.

NYPD vehicle mounted cameras do not contain any editing features, and the devices cannot be used to change recorded data. NYPD vehicle mounted cameras do not use any biometric technologies and cannot conduct facial recognition analysis.[2]

Additionally, both the NYPD's manned aircraft[3] and unmanned aircraft[4] systems are capable of recording video. However, those technologies differ from the devices covered in this impact and use policy in several ways and have been addressed in independent impact and use policies.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD's vehicle mounted cameras 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.

NYPD vehicle mounted cameras may only be used by NYPD personnel for legitimate law enforcement purposes. NYPD personnel operating vehicles equipped with dash-cams must activate long-term recording any time a vehicle stop is conducted.

NYPD personnel operating any vehicles equipped with a rear -facing interior camera must activate the camera any time a subject enters the passenger cabin of an NYPD vehicle.

Watercraft cameras are used by the NYPD's Harbor Unit to monitor crew and deck operations performed on NYPD watercraft. NYPD personnel operating watercraft equipped with watercraft cameras activate their BWCs when a job is assigned.

Any events for which recording is required must be recorded from start to finish.

Access to vehicle mounted cameras is limited to authorized operators of NYPD vehicles equipped with the technology. Prior to use of the vehicle mounted cameras, the operator must log in to the vehicle tablet. Vehicle mounted cameras only record what is occurring in real time and include an immutable timestamp. Prior to use of vehicle mounted cameras, the operator must check that the date and time on the device is correct.

Court Authorization: The NYPD does not seek court authorization to use vehicle mounted cameras. The devices only record law enforcement encounters occurring in locations that do not maintain a reasonable expectation of privacy.

Additional Guidelines: If an NYPD investigation involving political activity requires the use of vehicle mounted cameras, the Intelligence Division will use them in compliance with NYPD

[2] However, a still image can be created from the recorded video images and may be used as a probe image for facial recognition analysis. For additional information on the NYPD's facial recognition, please refer to the facial recognition impact and use policy.
[3] For additional information on the NYPD's manned aircraft systems, please refer to the manned aircraft systems impact and use policy.
[4] For additional information on the NYPD's unmanned aircraft systems, please refer to the unmanned aircraft systems impact and use policy.

policies. 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 vehicle mounted cameras 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 use of vehicle mounted cameras.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Physical Safeguards & Security Measures: Vehicles equipped with vehicle mounted cameras are stored at NYPD facilities when not in use, and the vehicle keys are secured within the facility. Additionally, a supervisor must periodically inspect and account for all NYPD vehicles equipped with vehicle mounted cameras. Access to vehicle mounted cameras is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty.

Data Safeguards & Security Measures: Recordings obtained from NYPD vehicle mounted cameras are retained within a cloud-based storage management system. Recordings may be downloaded to an NYPD computer or 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 systems will subject employees to administrative and potentially criminal penalties.

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

The dash-cams and rear facing interior cameras will record over a 60 second, video-only, "pre-event" buffer in a continuous loop. When the dash-cam or rear facing interior camera is activated via the "Event Button," automatic activation signal, or via vehicle tablet, the dash-cam and/or rear facing interior camera will then record audio and video until the recording is manually deactivated via the "Event Button" or vehicle tablet. The dash-cam and rear facing interior camera will then return to the buffering state, and the process is repeated. Completed recordings include the 60 second pre-event buffer period up to the moment of deactivation. Recordings cannot be paused or muted, only stopped.

NYPD dash-cams and rear facing interior cameras upload videos via secured wireless cellular or LTE signal post completion of recording to a cloud-based storage management system. Recordings relevant to a case or investigation will be stored in an appropriate NYPD computer or case management system.

All dash-cam and rear facing interior camera recordings uploaded to the cloud-based storage system must be assigned a category by NYPD personnel. All videos mirror the retention period for the BWC-recorded video(s) in the cloud-based storage system of at least 39 months. If the video is related to an arrest, it is then retained for 60 months (5 years). Watercraft cameras do not currently record.

NYPD vehicle mounted camera recordings may only be used for legitimate law enforcement purposes or other official business of the NYPD, including in furtherance of criminal investigations, civil litigation, and disciplinary proceedings. Recordings relevant to an investigation are retained within an appropriate NYPD computer or case management system. 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 computer and case management 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 recordings obtained from NYPD use of vehicle mounted cameras pursuant to the 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 NYPD vehicle mounted cameras.

If a vehicle mounted camera 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 from the NYPD in accordance with applicable laws and regulations, and NYPD policies. Additionally, the NYPD may provide retained recordings 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, recordings, 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 vehicle mounted cameras 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 vehicle mounted cameras 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 vehicle mounted cameras 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 assigned to the NYPD Highway Unit receive training in the technical use of dash-cams and the associated equipment. NYPD personnel who have access to vehicle mounted cameras receive command level training on the proper operation of the technology. Officers must operate all vehicle mounted cameras in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

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 the 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 recordings 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 vehicle mounted cameras. Additionally, after a search for relevant information, no physical safety hazards identifiable by manufacturer warnings or published academic research regarding physical safety hazards have been identified pertaining to the use of vehicle mounted cameras or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that vehicle mounted cameras 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 the impact and use policy for vehicle-mounted cameras mitigate the risk of partial and biased law enforcement. Vehicle mounted cameras only record what occurs within the cameras' field-of-view. Vehicle mounted cameras do not use any biometric measurement technologies. These devices are only deployed under supervisory review. Access is restricted to authorized personnel. Based on these safeguards, any theoretical risks of vehicle mounted cameras are effectively mitigated and do not result in disparate impacts.

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.