



BODY WORN CAMERAS: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT AND FINAL POLICY

Update	Description of Update
Removed statement that body worn 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 body worn camera capabilities.	Added language clarifying body worn camera capabilities. Added language describing how body worn cameras compliment other NYPD technologies.
Expanded upon body worn camera rules of use.	Added language clarifying body worn camera rules of use.
Expanded upon body worn camera safeguards and security measures.	Added language regarding information security. Added language to reflect the removal of access to body worn cameras when job duties no longer require access.
Expanded upon body worn camera data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws. Added language to reflect current NYPD policies and procedures relating to body worn camera retention.
Expanded upon body worn camera external entities section.	Added language to reflect NYPD obligations under the local privacy laws. Added language regarding access by federal court appointed monitor.
Grammar changes.	Minor syntax edits were made.

Date of Addendum	Addendum Description
November 24, 2023	Updated to reflect current NYPD body-worn camera policies.

BODY WORN 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

All uniformed members of the service below the rank of Deputy Inspector in the New York City Police Department (NYPD) are equipped with body-worn cameras (BWCs). The NYPD BWC program is the largest of its kind in the United States with over 29,500 members of the NYPD equipped with BWCs. BWCs are used to contemporaneously create an objective recording of a variety of encounters between the police and the public.

The NYPD produced this impact and use policy because BWCs have the ability to capture images of people, license plates, and any other visual or acoustic data within recording range of the cameras and share those recordings with NYPD personnel.

CAPABILITIES OF THE TECHNOLOGY

NYPD BWCs are manufactured by Axon. BWC are small battery-powered digital video cameras officers attach to the exterior layer of their uniform.

Once powered on, BWCs will record over a 60 second, video only, “pre-event” buffer in a continuous loop. This process is commonly referred to as “buffering.” When an officer activates the record switch, the preceding 60 seconds of video recording is automatically saved. That 60 second recorded video will not contain audio.

When the BWC is activated via the Event Button or automatic activation signal, the BWC will then record audio and video until the recording is manually deactivated via the Event Button. The BWC will then return to the buffering state,¹ and the process is repeated until the officer docks the BWC at the end of their tour. Completed recordings encompass the 60 second pre-event buffer period up to the moment of deactivation. Recordings cannot be paused or muted, only stopped.

BWCs provide empirical evidence through the contemporaneous creation of an objective audio and visual record of a variety of law enforcement encounters. BWCs are a vital tool in improving and enhancing the safety of officer and civilian interactions, in addition to evidence collection. BWC recordings facilitate review of events by supervisors, foster accountability, encourage lawful and respectful interactions between the public and the police, and may assist in de-escalation of possibly volatile encounters.

BWCs do not utilize any enhanced recording capabilities such as infrared, night vision, or varying degrees of view as (BWC have a fixed field of view. BWCs cannot be used to edit recorded videos. BWC activate automatically upon activation of an NYPD taser. Additionally, BWCs do not use video analytics or any kind of biometric measurement technology. BWCs do not use facial recognition technologies and cannot conduct facial recognition analysis.²

¹ Video recorded during the buffering state may not always appear in BWC video footage recorded during activation. For example, if an officer does not power on their BWC at the start of their tour and activates the BWC to record an incident, recorded video will only include what was recorded after BWC activation. Alternatively, if a BWC is deactivated and then is reactivated 15 seconds later, the buffering period will only consist of 15 seconds.

² However, a still image can be created from a BWC video recording and may be used a probe image for facial recognition analysis. For additional information on Facial Recognition, please refer to the facial recognition impact and use policy.

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

NYPD BWCs 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 BWCs may only be used by NYPD personnel for legitimate law enforcement purposes or official business. Officers must tell members of the public that they are being recorded unless the notification would compromise the safety of any person or impede an investigation. Officers do not need a person's permission to start, or to continue, recording.

Officers must activate their BWC prior to engaging in police action. Police action is defined as any police service, as well as law enforcement or investigative activity conducted in furtherance of official duties. Police action includes responding to calls for service, addressing quality of life conditions, handling pick-up assignments and any self-initiated investigative or enforcement actions such as witness canvasses, vehicle stops and Investigative Encounters. Routine consensual conversations with members of the public carried out as part of community engagement efforts are not considered police action.

Officers cannot record certain sensitive encounters, such as speaking with a confidential informant, interviewing a sex crime victim, or conducting a strip search.

Any events for which recording is required must be recorded from start to finish. If a member of the public asks an officer to turn off the camera, the officer may do so, but the officer may continue recording if the officer thinks it unsafe or inadvisable to stop after considering all the circumstances, including the requestor's desire for privacy and confidentiality. Except in limited circumstances, officers may not turn off the camera if a suspected perpetrator is still present on the scene.

At the end of a tour, officers must place BWCs in a docking station within a secure NYPD facility. The docking station is housed in a location inaccessible to the general public. Once docked, recorded videos are automatically uploaded to a cloud-storage system and the BWCs battery is recharged automatically.

Court Authorization: Court authorization is not sought prior to the NYPD's use of BWCs.

Additional Guidelines: NYPD investigations involving political activity are conducted by the Intelligence Division, which 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 BWCs 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 BWCs.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Physical Safeguards & Security Measures: BWCs 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 BWCs is limited to NYPD personnel with an articulable need to use the technology in furtherance of a lawful duty. Access to BWCs is determined by an officer's assignment and is rescinded when that officer's assignment no longer requires its use.

Data Safeguards & Security Measures: BWC-recorded video is encrypted both at rest on the device and in transit to the cloud-storage system. BWC-recorded video is uploaded to the cloud-storage system over a secured network. Access to the BWC-recorded video in the cloud-storage system is confidential-password-protected and is restricted to only authorized users.

BWC-recorded videos may be retained within appropriate NYPD computer or case management systems. 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

While powered, BWCs will record over a 60 second, video only, “pre-event” buffer in a continuous loop. When the BWC is activated via the Event Button or automatic activation signal, the BWC will then record audio and video until the recording is manually deactivated via the Event Button. The BWC will then return to the buffering state, and the process is repeated until the officer docks the BWC at the end of their tour. Once docked, recorded videos are automatically uploaded to a cloud-based storage system. Completed recordings encompass the 60 second pre-event buffer period up to the moment of deactivation. Recordings cannot be paused or muted, only stopped.

The BWC-video management system is confidential-password-protected, and access is restricted to only authorized users. Authorized users consist only of NYPD personnel in various commands. Authorized users may only access the BWC management system in order to execute their lawful duties; relating only to official business of the NYPD.

All BWC-recorded videos should be assigned a category by the NYPD officer that recorded the video. The category assignment sets the retention period for BWC-recorded video(s) within the cloud-based storage system. BWC-recorded videos categorized as ‘Homicide’ are never deleted and are retained indefinitely. BWC-recorded videos categorized as ‘Arrest’ are retained for five years. All other BWC recorded videos are retained for 39 months.

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. Videos are stored in the BWC-recorded-video management system utilized by the Department. NYPD personnel accessing the BWC-recorded-video management system are authenticated by username and password. Access to the management system 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 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 copies of BWC-recorded video through a Freedom of Information Law request. The NYPD will review and evaluate such requests in accordance with applicable provisions of the law.

In addition, the NYPD maintains a public release policy for “critical incidents.” A critical incident is any incident in which the following criteria is met:

1. Use of force by one or more officers that results in death or serious physical injury to another;
2. Officer discharges firearm and such discharge hits or could hit another; and/or
3. Any incident which the Police Commissioner determines the release of BWC footage will address vast public attention, or concern, or will help enforce the law, preserve peace, and/or maintain public order.

The NYPD decides when to publicly release BWC footage of a critical incident within 30 calendar days. The NYPD will release representative samples of the BWC video(s) depicting the critical incident, as well as any salient events leading up to the event. Extraneous and/or redundant material may be omitted. The footage will be redacted (e.g., faces of involved individuals may be blurred, etc.), as appropriate, prior to being released to the public. In the event that a federal and/or state prosecuting authority opens an official investigation into a critical incident, the NYPD will share all relevant BWC footage with the prosecuting authority within 24 hours of the NYPD being notified of the investigation. Unedited footage of a critical incident will be maintained, and released, to an appropriate investigating authority upon request.

The NYPD will notify the prosecuting authority 7 calendar days prior to releasing BWC footage of a critical incident to the public, except when the Police Commissioner determines that exigent circumstances require a shorter time period for such release (e.g., in order to maintain public safety, preserve the peace, etc.). In such cases, notice will be provided to the prosecuting authority 24 hours prior to releasing BWC footage of a critical incident to the public, if possible. When practicable, the release of BWC footage of a critical incident may occur at either a news conference, or media availability session, with a subject matter expert and an executive from the Office of the Deputy Commissioner, Public Information present to provide context and a chronology of the event. BWC footage may also be released on an online platform. BWC footage will not be released for commercial, non-law enforcement, or non-journalistic purposes.

EXTERNAL ENTITIES

In furtherance of judicial orders, the monitor appointed by the court in *Floyd, et al. v. City of New York* has access to the cloud-based BWC storage system to view BWC video. No other external entity has direct access to the information or data collected by the NYPD’s use of BWC.

If a BWC captures evidence related to a criminal case, the NYPD will turn the video over to the prosecutor with jurisdiction over the matter. Prosecutors will provide video to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request BWC-recorded video in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide the BWC-recorded video 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.

The NYPD provides the Civilian Complaint Review Board (CCRB) with BWC-recorded video in furtherance of investigations of alleged incidents of misconduct under their jurisdiction. BWC-recorded video provided to CCRB may be redacted to protect confidential information or comply with relevant statutes including the sealed records laws (e.g. Criminal Procedure Law section 160.50 – 55) which generally prohibit the release of certain records absent a court order or consent of the individual(s) depicted.

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 BWCs 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 BWCs 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 BWC-recorded video is 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 equipped with BWCs receive classroom and practical training on the proper operation of the device and the associated equipment. NYPD personnel must operate any BWC and its associated equipment in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

The NYPD has multi-tiered levels of review and engages in self-initiated review to ensure that officers are properly using BWCs and recording when required. Sergeants review and document a sampling of police officers' footage monthly, which is then reviewed by lieutenants within the command, followed by review from the executive officer. Once approved, those documents which contain the reviewed files, are sent to the Professional Standards Division, Compliance Section, BWC Unit (BWC Unit). The Integrity Control Officers (ICOs) within each Command send a monthly certification to the BWC Unit confirming this review has been completed. Upon receiving the files, the BWC Unit review and log the documents for completeness.

In addition, BWC compliance analysis is incorporated into assessments by the BWC Unit and Compliance Stat. The BWC Unit conducts visits to commands experiencing compliance issues to reinforce policy and address any procedural questions. The BWC Unit also informs the commands when the unit identifies a mandatory activation incident that was not recorded. The Patrol Supervisor is mandated to investigate the incident and report back to the BWC Unit with their findings, including disciplinary action taken. The BWC Unit also informs commands of their compliance rates so commands can track their compliance.

All 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).

Supervisors of personnel utilizing BWCs 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.

ICOs 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 body worn 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 body worn cameras or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY & IMPACT & USE POLICY

The NYPD has implemented significant safeguards to ensure that body worn 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 this impact and use policy for BWCs mitigate the risk of partial and biased law enforcement. NYPD utilization of BWCs does not integrate the use of video analytics, facial recognition or any other biometric measurement technology. Based on these safeguards, any theoretical risks of body worn 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.