CASE MANAGEMENT SYSTEMS: IMPACT AND USE POLICY

UPDATED: FEBRUARY 4, 2026

SUMMARY OF CHANGES BETWEEN DRAFT & FINAL POLICY

Update	Description of Update
Removed statement that case management systems 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 case management system capabilities.	Added language clarifying case management system capabilities. Added language describing how case management systems compliment other NYPD technologies.
Expanded upon case management system rules of use.	Added language clarifying case management system rules of use.
Expanded upon case management system safeguard and security measures.	Added language regarding information security. Added language to reflect the removal of access to case management systems when job duties no longer require access.
Expanded upon case management system data retention.	Added language to reflect NYPD obligations under federal, state, and local record retention laws.
Expanded upon case management system external entities section.	Added language to reflect NYPD obligations under the local privacy laws.
Grammar changes.	Minor syntax edits were made.

CASE MANAGEMENT SYSTEMS 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

Case management systems enable New York City Police Department (NYPD) personnel to organize and store the voluminous records obtained during the course of official investigations and operations. Case management systems are an efficient, sustainable, and cost-effective replacement to paper-based case management methods.

The NYPD produced this impact and use policy because NYPD case management systems organize, retain and, when appropriate, share a variety of records and evidence connected to official investigations and operations. This includes but is not limited to: video images, acoustic data, possible location information, and photographs of individuals.

CAPABILITIES OF THE TECHNOLOGY

Maintenance of paper records is expensive, considering storage space, mailing fees, as well as the time allocution needed for NYPD members to transport, store, track, and retrieve records, and locate lost or misfiled records. Case management systems allow the NYPD to electronically store and organize records and information obtained in the course of investigations and operations in a central location.

NYPD case management systems are manufactured by SoundThinking, Inc. These systems may be used in conjunction with the NYPD's data analysis tools[1] to provide NYPD investigators with information that would otherwise be kept throughout different isolated data compartments within NYPD computer systems. Records can be efficiently and repeatedly accessed in support of law enforcement operations.

NYPD case management systems do not use any biometric measuring technologies. NYPD case management systems do not use facial recognition technologies and cannot conduct facial recognition analysis.[2]

RULES, PROCESSES & GUIDELINES RELATING TO USE OF THE TECHNOLOGY

Case management systems 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 case management systems may only be used by NYPD personnel for legitimate law enforcement purposes. All information contained in NYPD case management systems are subject to privacy, confidentiality, and dissemination restrictions according to NYPD policy and applicable federal, state, and local laws and rules. All members of the NYPD must only access case management systems to which authorization has been granted and under circumstances required in the execution of lawful duty relating to official business of the NYPD.

[1] For additional information on data analysis tools, please refer to the data analysis tools impact and use policy.
[2] However, still images within the systems may be used as a probe image for facial recognition analysis. For additional information on facial recognition, please refer to the facial recognition impact and use policy.

Court Authorization: Court authorization is not required prior to NYPD use of case management systems. Case management systems are a digital storage tool used to organize information lawfully obtained by NYPD personnel.

Additional Guidelines: If an NYPD investigation involving political activity requires the use of case management systems, the Intelligence Division will use it in compliance with Department 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 case management systems 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 case management systems.

SAFEGUARD & SECURITY MEASURES AGAINST UNAUTHORIZED ACCESS

Data Safeguards & Security Measures: Case management systems are confidential-password-protected. Access is restricted to only authorized users. Differentiated 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. Authorization must be requested by a Commanding Officer. Authorization requests receive several layers of executive review. Access levels are only granted for functions and abilities relevant to individual commands. Case management system access levels are determined by an officer's assignment and are rescinded when that officer's assignment no longer requires its use.

NYPD personnel must abide by security terms and conditions associated with NYPD computer and case management systems, including those governing user passwords and logon procedures. Members of the NYPD 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 utilizing case management systems are authenticated by username and password. Access to case management 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 systems is 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 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

Data contained within NYPD case management systems may only be used for legitimate law enforcement purposes or other official business of the NYPD, including the furtherance of criminal investigations, civil litigations, and disciplinary proceedings. NYPD personnel utilizing computer and case management systems are authenticated by username and password. Access to computer and case management 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.

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 information contained with a NYPD case management system 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 information contained within NYPD case management systems 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

Some prosecutorial agencies have limited access to case management systems data through Department controlled disclosures. The department selectively shares relevant information and data on a case-by-case basis in accordance with applicable laws, discovery obligations, and NYPD policies. Prosecutorial agencies do not have access to the information or data contained in ECMS other than what is proactively shared pursuant to relevant law or policy.

Information contained within NYPD case management systems is often related to criminal investigations. When an investigation results in an arrest, the NYPD turns over relevant information to the prosecutor with jurisdiction over the matter. Prosecutors will provide the information to the defendant(s) in accordance with criminal discovery laws.

Other law enforcement agencies may request information contained in NYPD case management systems in accordance with applicable laws, regulations, and New York City and NYPD policies. Additionally, the NYPD may provide information contained with NYPD case management systems 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, information contained in NYPD case managements systems 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, members of the NYPD 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 case management systems 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 case management systems 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 information contained within NYPD case management systems 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 using a NYPD case management system receive command-level training on the proper operation of the technology and associated equipment. NYPD personnel must operate case management systems in compliance with NYPD policies and training.

INTERNAL AUDIT & OVERSIGHT MECHANISMS

Immutable audit logs are created when any information is searched or accessed through any case management system. The log-in and use of the system is traceable to a particular user and periodically audited for misuse by the precinct or unit's Commanding Officer. Allegations of misuse are internally investigated at the command level or by the Internal Affairs Bureau (IAB).

All members of the NYPD are advised that NYPD case management systems are intended for the purposes of conducting official business. The misuse of any system will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by 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 case management systems. 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 case management systems or associated equipment.

DISPARATE IMPACTS OF THE TECHNOLOGY

The NYPD has implemented significant safeguards to ensure case management systems 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 NYPD case management systems mitigate the risk of partial and biased law enforcement. NYPD case management systems are a digital organizational and storage tool for information and evidence that would be too voluminous and uneconomical to store through maintenance of paper records. Access is restricted to authorized personnel. NYPD case management systems do not use any kind of biometric measuring technologies. Based on these safeguards, any theoretical risks of case management systems 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.